Computer Networks 90 (2015) 49–73

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Trust management and reputation systems in mobile participatory sensing applications: A survey

Hayam Mousa[a,b,*], Sonia Ben Mokhtar[a], Omar Hasan[a], Osama Younes[b], Mohiy Hadhoud[b], Lionel Brunie[a]

[a] LIRIS, INSA de Lyon, France
[b] Faculty of Computers & Information, Menoufia University, Egypt

ARTICLE INFO

Article history:
Received 30 October 2014
Revised 13 June 2015
Accepted 3 July 2015
Available online 30 July 2015

Keywords:
Participatory sensing
Vulnerabilities
Trust systems
TPM
Reputation
Challenges

ABSTRACT

Participatory sensing is an emerging paradigm in which citizens everywhere voluntarily use their computational devices to capture and share sensed data from their surrounding environments in order to monitor and analyze some phenomenon (e.g., weather, road traffic, pollution, etc.). Interest in participatory sensing systems has risen since a large mobile sensor network can now be opportunistically constructed with much less cost and effort than it was the case a decade ago. However, relying on citizens who share their contributions raises many challenges. Participants can disrupt the system by contributing corrupted, fabricated, or erroneous data. Consequently, monitoring the participants' behavior in order to estimate their honesty is an essential requirement. This enables to evaluate the veracity and accuracy of participants' contributions and therefore, to build robust and reliable participatory sensing systems. Recently, several trust and reputation systems have been proposed to trace participants' behavior in these systems. This survey presents a study and analysis of existing trust systems in participatory sensing applications. First, we study the nature of participatory sensing applications by surveying existing systems and outlining their common features. We then analyze the main vulnerabilities and attacks that can be launched in these systems. Furthermore, we discuss the concept of trust and we introduce a classification of existing trust systems. The two main classes of trust assessment methods for participatory sensing (i.e. Trusted Platform Module and reputation) are discussed. In addition, we analyze the merits as well as the limitations of each of them. We then derive a comparative study of several existing trust systems for participatory sensing. From this study, we identify many trust problems that have not been solved and many attacks have not been addressed yet in the literature. Finally, we list future research directions regarding trust management in participatory sensing systems.

1. Introduction

Everyday, millions of people move around carrying a variety of handheld devices equipped with sensing, computing, and networking capabilities (e.g., smartphones, tablets, music players, GPS watches, in-vehicle sensors, etc.) [1]. The advancement and widespread use of such devices have contributed toward the emergence of a new kind of application called *participatory sensing* [2]. These applications exploit both the mobility of participants and the sensing capabilities of their devices to construct opportunistic mobile sensor networks [3].

In participatory sensing, participants capture sensed data from their surrounding environment using a variety of

[*] Corresponding author. Tel.: +33 652 183 950.
E-mail addresses: hayam910@gmail.com, hayam.kafaky@insa-lyon.fr (H. Mousa), Sonia.Benmokhtar@insa-lyon.fr (S.B. Mokhtar), Omar.Hasan@insa-lyon.fr (O. Hasan), osama.younes@ci.menofia.edu.eg (O. Younes), mmhadhoud@ci.menofia.edu.eg (M. Hadhoud), Lionel.Brunie@insa-lyon.fr (L. Brunie).

http://dx.doi.org/10.1016/j.comnet.2015.07.011
1389-1286/© 2015 Elsevier B.V. All rights reserved.

sensors (e.g., GPS, camera, microphone, accelerometer, gyroscope, digital compass, etc.) embedded in their devices. Then, they share their collected observations with a backend server, which processes the received data to monitor, map, or analyze some incidents or phenomena of common interest.

Participatory sensing systems can be applied to serve many of our daily life needs, including health monitoring (e.g., [4–8]), traffic monitoring (e.g., [9–12]), noise monitoring (e.g., [6,13,14]), weather monitoring (e.g., [6,15]), activities monitoring [16–20], commerce [21,22], sports monitoring [23], as well as other applications [24].

In these applications, no restrictions are usually imposed about the participants' experience, concern, trustworthiness, and interest. In addition, they are not usually paid for their participation in the sensing campaign. Thus, they usually do not have strong motivations to comply with the tasks' requirements. That is, they are not concerned about some parameters which may improve the quality of their contributions (e.g. time, location and/or the position of the device during the sensing process). As a consequence, participatory sensing applications are vulnerable to *erroneous* and *malicious* participants. We define erroneous and malicious participants as those who mislead and disrupt the system measurements by reporting false, corrupted or fabricated contributions either intentionally or non-intentionally. Non-intentional (i.e. erroneous) corruption may originate from a malfunctioning sensor while intended (i.e. malicious) corruption is deliberately committed to alter the system measurements in a specific location. For instance, an adversary can put his device in a non-appropriate position. Alternatively, the participant can modify a contribution before sharing it. Malicious participants may further launch various types of attacks such as Sybil, collusion, on-off attack, etc. These attacks are discussed in Section 3. Consequently, the need arises for approaches that try to detect erroneous participants and deter or mitigate malicious ones in order to evaluate the veracity and accuracy of participants' contributions and therefore to build robust and reliable application systems [25,26].

Among the classical solutions to deal with erroneous and malicious users is the notion of *trust* [27]. Trust systems aim to estimate the trustworthiness of entities' behavior. Some of these systems depend on the *reputation* of entities for assessing their trust. Reputation is defined as the aggregated opinion of the community members about how much the behavior of the target entity is trusted [28]. Assessing the trust and reputation of entities permits the system to evaluate their expected behavior for their future interactions.

Indeed, trust and reputation systems have been studied and applied in different domains such as peer-to-peer networks (e.g., [29]), ad-hoc networks (e.g., [30–32]), wireless sensor networks (e.g., [33–35]), etc. In the context of participatory sensing, evaluating participants' reputation enables for assessing the trust of their provided contributions.

Trust and reputation systems are also vulnerable to malicious adversaries. Those adversaries try to disrupt and mislead the decisions of reputation systems. In addition, some reputation systems adopt incentive mechanisms to motivate participants to join sensing campaigns. Such systems are vulnerable to selfish adversaries who try to gain higher reputation scores or more incentives than they merit [36,37].

In complement to reputation-based trust systems, researchers have suggested to equip smartphones with an embedded trusted platform module (*TPM*) [38,39]. Such a module ensures the authenticity of participants' contributions. Furthermore, some TPM-based systems can protect data from unauthorized access through applying some authentication and hardware cryptography mechanisms.

Although, TPM solutions have some merits, they also suffer from a number of limitations. A major limitation of TPM-based solutions is that they only consider data authenticity and protection regardless of the participant's sincerity and honesty [40]. TPM cannot detect contributions from malicious participants who deliberately initiate sensing actions that cause distortion of their contributions. For example, in a noise monitoring application, a participant may intentionally put his device inside a bag. In a weather monitoring application, a participant can put his device beside a fireplace or inside a refrigerator. Consequently, the need arises for solutions to take into consideration additional parameters related to the participants' behavior and honesty. These parameters may include participants' reputation, knowledge, experience, etc.

In this paper, we survey existing research efforts for trust assessment in participatory sensing applications belonging the two major categories above which are reputation-based and TPM-based trust systems.

1.1. Contribution

The contributions of this paper can be summarized as follows:

- We present an overview of participatory sensing, a classification of its applications and a classical architecture for sensing campaigns [24,41].
- We analyze the vulnerabilities of these systems and list a set of attacks that can be launched in these systems. We further propose a threat model that classifies these attacks.
- We recall the definition of trust in the context of participatory sensing and propose a classification of trust systems in this context.
- We discuss different methods of trust assessment such as reputation and TPM systems. We define the goals, components, and functions of these methods.
- We survey state-of-the-art trust systems for participatory sensing and carry out a multi-criteria comparative study of these systems. We perform this comparison according to the parameters of the analysis framework.
- Finally, we draw the main directions of research in trust assessment for participatory sensing applications.

1.2. Organization

The remainder of this paper is organized as follows. First, we present an overview about participatory sensing systems in Section 2. Then, we discuss different attacks and propose a threat model for these systems in Section 3. In Section 4, we discuss the notion of trust and propose a classification of existing trust systems. In Sections 5 and 6, we present a detailed discussion of the two main classes of trust systems. In addition, the state-of-the-art of trust systems are surveyed in Section 7. We then present a comparative study and analysis of the surveyed systems in Section 8. Finally, we explain open research challenges in Section 9, present the related work in Section 10, and conclude the paper in Section 11.

2. Participatory sensing

In the following subsections, we present the fundamentals of participatory sensing.

2.1. Participatory sensing applications

Participatory sensing applications have a nature similar to some other types of network based applications such as crowdsourcing. Crowdsourcing is defined in [42,43] as the process of obtaining needed services, ideas, or content by soliciting contributions from a large group of people, and especially from an online community, rather than from traditional employees or suppliers. In crowdsourcing, participants usually have some motivation for participation (e.g. money, altruism, fun, reputation, and/or learning). Participants may perform any computational task. In addition, they can join crowdsourcing campaigns from any fixed or mobile device. Moreover, crowdsourcing systems usually adopt some incentives and reward mechanisms.

However, participatory sensing has some particularities that differentiate it from these applications. One difference is that participants are usually volunteers; they are not usually paid for their participation. In addition, they should have handheld computational devices with some sensing capabilities to join the sensing campaigns. Moreover, incentives and rewards are not usually available. More details about the differences between participatory sensing and other applications are described in detail by Ganti et al. in [44]. Here, we focus on participatory sensing because participants in such environments usually lack a strong motivation to comply with the tasks' requirements (e.g. putting their device in the correct position). Thus, these systems are much more vulnerable to misbehaved participants.

Khan et. al. in [24] classify participatory sensing applications into three main categories: *public*, *personal* and *social* centric participatory sensing. In public sensing applications, participants use their mobile phones to collect data and observations about their surrounding environment such as noise, traffic, pollution, etc. [6,9,45–47]. Personal sensing applications are those in which the sensing is based on monitoring the participants themselves such as their health status, activities, etc. [48–52]. In social participatory sensing, participants share sensed data with their friends [53], which can provide them higher motivation for contributing their resources to participatory sensing.

2.2. Architecture of a participatory sensing system

Most of participatory sensing systems mentioned above share the client-server architecture presented earlier in [41] and depicted in Fig. 1. In this architecture, we can distinguish three main parties: participants (depicted at the bottom of the figure), a campaign administrator (depicted in the middle of the figure) and end users (depicted at the top of the figure). In the following steps, we show how different parties interact to accomplish a sensing campaign according to this architecture:

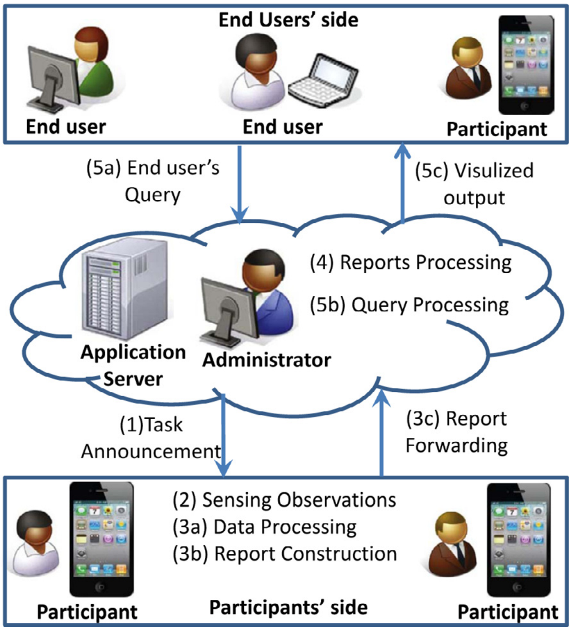


Fig. 1. Typical architecture of a participatory sensing system.

1. ***Task announcement***: The campaign administrator initiates the participatory sensing campaign, manages the campaign and setups the application server. Tasks are then announced to the participants through the application server (step 1).
2. ***Sensing observation***: Each participant selects one or more tasks and uses his own device to capture his observations (step 2).
3. ***Reports preparation***: Once the participant finalizes capturing the required samples, local processing is carried out on the sensed data (step 3a). Local processing summarizes sensed data, extracts some high-level information from the data, and/or applies some privacy protection mechanisms. Next, one or more sensing reports are constructed (step 3b). Finally, the participant's device uses the available communications network to send these reports to the application server (step 3c).
4. ***Report processing***: The received reports are maintained by the application server. Reports received from different participants for the same task are stored in the related database. Subsequently, reports are processed and analyzed in order to extract the required features and measurements (step 4).
5. ***End user query***: The end user sends a query to the server (step 5a). The server processes the query (step 5b), and returns the result to the user (step 5c).

3. Vulnerabilities of participatory sensing applications

One of the major limitations of participatory sensing systems is the uncertainty of participants' behavior. In addition, there is a lack of incentives that can encourage participants to comply with the requirements of the sensing tasks. Therefore, these systems are vulnerable to erroneous contributions as well as to contributions from malicious participants. In the following subsection, we discuss a framework of different attacks faced by participatory sensing applications. Then, we propose a threat model to describe how these vulnerabilities affect the system.

3.1. Attacks on participatory sensing applications

In this section, we present a set of well-known attacks in networked applications (e.g., [29,54–57]) and discuss how they apply to participatory sensing applications [25].

- ***Corruption attack***: This attack may arise as a result of a malfunctioning sensor of a participant's device. In addition, the adversary can deliberately contribute corrupted or forged data. Furthermore, a local processing module can also be used by the adversary for modifying the sensed data before sharing it. Moreover, an adversary can initiate sensing actions which may corrupt the sensed data by putting his device in non-appropriate positions. The system should have strong capabilities to identify correct contributions in order to identify and exclude corrupted ones.
- ***On-off attack***: In this attack, the adversary alternates between normal and abnormal behaviors. Specifically, the adversary provides false data randomly and irregularly with a probability p. The adversary can keep his trust above the required threshold by alternating his behavior as required. This makes it difficult to be detected [58–60]. To defend against this attack, the system should keep the history of participants besides a good capability to define their instantaneous trust. The behavior of an on-off adversary is usually unstable along time.
- ***Re-entry attack***: An adversary who has a low trust level decides to leave the system and to rejoin it using different identification parameters. This attack enables an adversary to contribute low quality or corrupted data and to avoid the consequences for such misbehavior. This attack is also referred to as *Newcomer* or *White Washing* attack [57,61,62]. The resistance against this attack depends on the strength of the adopted authentication mechanism. That is the same participant should not have the ability to obtain multiple identification parameters concurrently.
- ***Discrimination***: Participants can simultaneously join different sensing campaigns each of which is concerned with a specific phenomenon (e.g. weather, pollution, noise, etc.) [63–65]. An adversary commits a discrimination attack when he has a selective behavior towards different campaigns. The adversary provides high-quality contributions to some campaigns whereas he provides low-quality ones to other campaigns. To defend against such attack, trust systems should consider the user who is involved in different campaigns. However, trust systems are usually concerned with only one specific campaign. This makes it difficult for the current trust system to defend against such an attack.
- ***Collusion attack***: Multiple malicious participants acting together can cause more damage than each one acting independently. This attack is referred to as a collusion attack. Malicious colluding participants coordinate their behavior in order to provide unified false, corrupted contributions, and/or false feedback [66]. If the majority of participants collude they can mislead the system measurements and decisions. In order to attain robustness against such attack, systems should not rely on consensus algorithms to define good and bad contributions. Otherwise, the system measurements and decisions will be biased if collusion is committed.
- ***Sybil attack***: Some participatory sensing systems apply authentication mechanisms. However, a single participant may have the ability to generate multiple pseudonymous identities. For instance, the system, presented by Wang et al. [37] uses a blind signature for authenticating participants. However, participants can generate different identification parameters. Subsequently, an adversary has the ability to submit multiple sensing reports for the same task or to submit many feedback reports for the same participant [37,67,68]. This behavior corrupts the system measurements and misleads the trust system decisions. The Sybil attack is studied earlier in [69–72]. The difference between Sybil and re-entry attack is that multiple pseudonyms are synchronized to login into the system. Similarly, systems should adopt strong authentication mechanisms to defend against Sybil attacks.
- ***Reputation lag exploitation***: There is usually a time lag between the instant when a sensing report is submitted and the instant when the evolution of this report is reflected on the corresponding trust rating of a participant. Consequently, malicious participants have the chance to contribute corrupted data by exploiting this lag. For instance, an adversary initially provides good quality contributions for some period of time in order to gain a high trust rate. The adversary then misuses this trust by injecting the system with corrupted reports [56]. To defend against such attack, systems should have the ability to trace the instantaneous behavior of participants. Thus, the evolution of their behavior should instantaneously reflect in their trust scores.
- ***GPS spoofing***: Another set of attacks was defined in [36]. These attacks target to tamper with the sensing campaign through reporting an inaccurate location information. The adversaries spoof their locations on the phone by using some applications (e.g. FakeLocate). Then, they report false information by letting the participatory sensing application know that they are in the sensing area, when in reality they are not [73,74].

The previous attacks can all be implemented to affect either the application or the trust and reputation systems. The following attacks target only the reputation system in which users are permitted to provide a feedback about participants' contributions. Thus, the following attacks usually have an indirect effect on the application measurements:

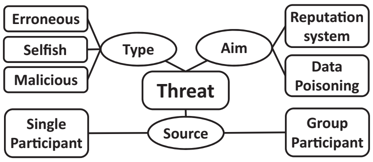


Fig. 2. Threat model of the participatory sensing attacks.

- ***Unfair ratings***: The adversary rater does not report an accurate feedback which reflects his genuine opinion about the participant [56,75–78].
- ***Bad mouthing attack***: This attack arises when the rater provides a negative feedback rating for a trusted participant. This attack is also referred to as *false accusation* attack [79,80].
- ***Ballot stuffing attack***: The adversary may assign a positive feedback to misbehaved participants. This attack is also referred to as *false praise* attack [34,81].
  To defend against such attacks, trust systems should incorporate a methodology to evaluate the aggregated feedback in order to mitigate the effect of such attacks.

3.2. Threat model

In view of the above-described attacks, we propose a threat model presented in Fig. 2 to describe different forms of vulnerabilities and attacks in participatory sensing systems. We propose to analyze attacks along the following dimensions:

Type. A threat can originate from different types of participants: *erroneous*, *malicious*, and *selfish* participants. Erroneous contributions may be a result of a malfunctioning hardware or software held by a participant. Malicious participants may deliberately report false, corrupted, or forged sensed data in order to disrupt the application analysis and measurements. While malicious adversaries offer their contributions without concern to the task requirements. In addition, selfish adversaries arise with the systems which adopt some incentive mechanisms [36,37]. Selfish adversaries attempt to increase their utility (e.g. coupons, rewards, quotas, receipts). Alternatively, they try to double spend their quotas. They can also launch reputation-based attacks in attempt to gain higher reputation scores and subsequently more incentives.

Source. An attack can be initiated either from a *single* participant or from a *group* of participants. In a single source attack, a single participant either provides a bad data or reports an inaccurate feedback. However, in a group source attack, a group of participants coordinates their behaviors to achieve some malicious goals by providing unified bad data or reporting unified unfair feedback. Thus, they can significantly disrupt the system measurements and decisions. It is, of course, more difficult to detect and treat attacks originated from a group of adversaries.

Aim. An attack may disrupt the system by sharing erroneous, corrupted, and fabricated data (i.e., *data poisoning attack* in the figure). Other attacks try to disrupt the reputation system by providing unfair ratings about other participants (i.e., *reputation system attack* in the figure). Reputation-based attacks make a trust system assigns low trust scores for honest participants and high scores for dishonest ones. Thus, contributions of honest participants are considered less important and vice versa. Subsequently, data poisoning attacks directly affect the system, while reputation-based attacks indirectly affect the measurements of the application system.

In Table 1, we classify the attacks discussed at the beginning of this section according to the dimensions of our proposed threat model. It is clear that only corruption attack can be erroneous (e.g. a result of malfunction sensor). Collusion, Sybil, unfair, bad mouthing, and ballot stuffing attacks do not result in a direct benefit to the adversary. However, they can only indirectly bias the system decisions in favor of the adversary. Thus, they can gain more rewards and incentives. Therefore, these attacks can be classified under selfish behavior. While a malicious adversary intends to disrupt the system, he can launch any of the other attacks as well. It is evident also that, all attacks are single source except collusion which is usually launched through the coordination between multiple adversaries. We can deduce also that collusion, Sybil, unfair rating, bad mouthing, and ballot stuffing attacks can target the disruption of the reputation system decisions. While corruption, on-off, re-entry, discrimination, collusion, Sybil, reputation lag, and GPS spoofing target to disrupt the collected data (i.e. data poisoning attack).

Table 1
Attacks classification according to the proposed threat model.

Attacks/dimensions	Type			Source		Aim	
	Erroneous	Selfish	Malicious	Single	Group	Reputation system	Data poisoning
Corruption	√	–	√	√	–	–	√
On/off	–	–	√	√	–	–	√
Re-entry	–	–	√	√	–	–	√
Discrimination	–	–	√	√	–	√	√
Collusion	–	√	√	-	√	√	√
Sybil	–	√	√	√	–	√	√
Reputation lag	–	–	√	√	–	–	√
GPS spoofing	–	–	√	√	–	–	√
Unfair rating	–	√	√	√	–	√	–
Bad mouthing	–	√	√	√	–	√	–
Ballot stuffing	–	√	√	√	–	√	–

Recently, trust systems have been adopted to resist or mitigate the effect of the existence of such attacks. In this paper, we survey and analyze these trust systems.

4. Classification of trust systems in participatory sensing

In participatory sensing, participants can tamper with their observations before submission in different ways as discussed in Section 3.1. Subsequently, participants' honesty and veracity determine the reliability of their contributions. Thus, assessing the expected behavior of a participant can help to assess the reliability of his contributions. That is, the quality of a provided contribution reflects the behavior of its provider.

In [82], we discussed and compared different definitions of trust. However, in the context of participatory sensing, trust relates more to the quality and reliability of participants' contributions. Thus, trust of a contribution is defined as the probability of the contribution being correct, as perceived by the application server [37].

For assessing the trust of participants and their contributions, different trust systems have been proposed in participatory sensing. These trust systems also seek to resist and/or mitigate the effect of the attacks discussed in Section 3.1. We have studied these systems to define their features. Thereafter, in the following subsection, we introduce a new classification framework and discuss the advantages and disadvantages of each of the proposed classes.

The framework of our classification of trust systems in participatory sensing is based mainly on three dimensions including the *methodology* of the trust assessment system, the *distribution* employed, and the *anonymity* assumed for the participants involved in the sensing campaign, as depicted in Fig. 3.

4.1. Methodology

Trust systems can be classified according to the methodology used for trust assessment. Some systems depend on the existence of a trusted platform module (*TPM*) while other systems try to assess the trust based on the *reputation* of participants. TPM is a hardware chip that ensures the authenticity of a participant's contribution by signing it (e.g. [38]). More details about how TPMs manage trust are presented in Section 5.

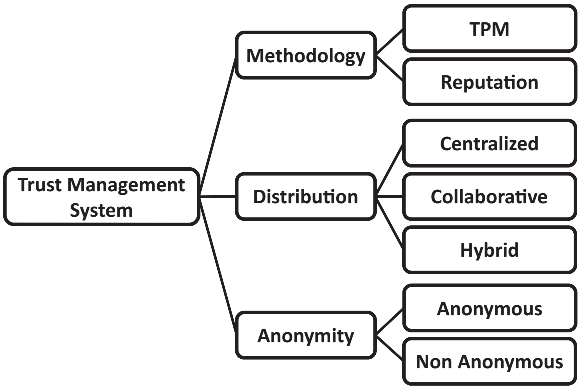


Fig. 3. Classification of trust systems in participatory sensing.

Alternatively, in reputation-based trust systems, participants' behavior is the primary measure of their trust. Participants who are witnessed to have a good behavior are assigned higher reputation and trust scores. An example of reputation-based trust system is presented in [83]. In this system, each participant is assigned a reputation score which reflects the quality of his current contribution. Additionally, the reputation score and the old trust score, which were previously assigned to a participant, are integrated to compute a new trust score for this participant. The full process of assessing trust through reputation systems is discussed in Section 6.

We discuss the strengths and weaknesses of TPM and reputation-based systems in Sections 5.4 and 6.3 respectively.

4.2. Distribution

A trust system can be constructed as centralized, collaborative, or hybrid. Some trust systems exploit the existence of a trusted central third party referred to as *trust server* (*trust manager*). This type of system is called *centralized* trust system. In these systems, trust scores are maintained and stored by a trust server. The trust server receives both the participants' contributions and users' feedback. It then evaluates the contributions and aggregates the feedback to calculate a trust score for each participant. It also disseminates these scores to the users. A detailed discussion of some instances of these systems are presented in Section 7.1.

In some cases a participatory sensing application allows a node to act as a source and a sink at the same time. Each node receives the others' contributions while sharing its own ones. In such systems, trust maintenance and storage are equally distributed over all the nodes in the system. These systems are referred to as *collaborative* trust systems. In these systems, there is no central trusted authority. Each entity receives the other participants' contributions, evaluates these contributions, aggregates the neighbors' opinion about the target entity, and calculates a trust score for the target entity. Each node then disseminates the calculated trust scores to be exploited by the others. In Section 7.2, we introduce several examples of collaborative trust systems.

In some other systems, the application server is responsible for trust assessment. In these systems, there is no central trusted third party. The application server itself uses its own evaluation of participants' contributions and/or users' feedback to assign trust scores to those participants. Each application server manages the trust scores of the participants involved in its own campaigns. We refer to these systems as *hybrid* trust systems. In hybrid systems, the application server simultaneously hybridizes/incorporates the role of both trust and application servers. One of these systems is presented in [84]. In this system, the application server measures the consistency of a participant's contribution compared with the other contributions for the same task. It then assigns a trust score to each participant. In Section 7.3, we discuss various hybrid trust systems.

4.2.1. *Merits and limitations of different distributions*

Concerning centralized trust systems (e.g. [85–89]), the existence of a central authority confirms that information collection, aggregation, and dissemination are maintained correctly. Additionally, they are resistant to some types of attacks such as Sybil and collusion attacks. Furthermore, a minimal overhead is imposed on the participants' devices, which often have computation and energy limitations. However, the central authority must be available and correct at all times. Thus, centralized trust systems are vulnerable to a single point of failure problem. Moreover, the central server imposes some limitations on the system's scalability.

The limitations of centralized systems can be avoided by employing collaborative trust systems (e.g. [90,91]). Nevertheless, collaborative systems impose extra overhead on every entity in the system. Hybrid trust systems seek to find a balance between scalability and the overhead distribution among the application server and the participants (e.g. [36,37,92]).

4.3. *Anonymity*

In participatory sensing campaign, participants share their sensitive data such as their location information [41]. As discussed before, they do not have some strong motivations to encourage them join sensing campaigns (e.g. no remuneration for participation). Thus, participants are inhibited to join these campaigns if they are asked to contribute their sensitive data without the assurance of strong privacy guarantees [26]. For this, trust systems that preserve participants' anonymity can be constructed. Preserving the participants' anonymity encourages them to share their personal information without being concerned about identity leakage (e.g., [68,89]). In [68], Wang et al. adopt a blind signature module for anonymity preservation. In [89], Huang et al. suggest using multiple pseudonyms for the same participant such that the participant uses a new unlinkable pseudonym each time. In this system, the server is responsible for pseudonym management.

In the following sections, we focus on the methodology dimension of the proposed classification since we are interested in how trust can be assessed within participatory sensing through different methodologies (i.e. TPM and reputation-based trust systems).

5. Trusted platform module (TPM)

Trusted platform modules (TPMs) are hardware chips that reside on participants' devices. Among other goals, TPMs ensure that the data sensed by a mobile sensor and reported to an application server are indeed captured by authentic and authorized sensor devices within the system. Thus, TPMs assure data authenticity as described in [93,94]. In the following subsection, we describe some of the components of a TPM module.

5.1. *TPM components*

As depicted in Fig. 4,[1]. a TPM comprises of several components [93,94]. These components include:

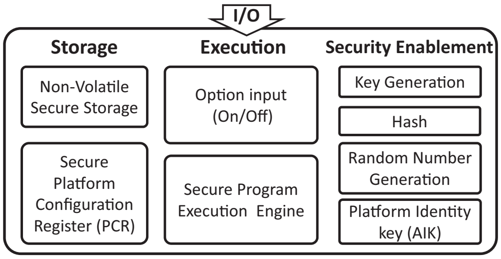

I/O
Storage
Execution
Security Enablement
Non-Volatile Secure Storage
Secure Platform Configuration Register (PCR)
Option input (On/Off)
Secure Program Execution Engine
Key Generation
Hash
Random Number Generation
Platform Identity key (AIK)

Fig. 4. TPM module.

- ***Non-volatile secure storage***: A TPM stores the information required for authentication such as passwords, certificates, and/or encryption keys. This information needs to be stored securely over long periods of time. Therefore, such information is stored in a non-volatile secure storage.
- ***Secure platform configuration registers***: Platform configuration registers (PCR) is the storage in which the sensed data are stored.
- ***Hash:*** A cryptographic hash module is used to calculate a hash value for the data that are going to be loaded in the PCR. The hash value is then appended to the data itself and loaded altogether in the PCR.
- ***Platform identity key***: The private key of a TPM is stored in a separate storage. It is referred to as attestation identity key (AIK).
- ***Secure program***: The execution engine of a TPM which executes one or more of the TPM required functions.
- ***Key and random number generator components***: A TPM can include components for generating keys and random numbers. Both keys and random numbers are exploited by the TPM to perform different functions carried out through the secure program.
- ***Option input (On/off)***: The TPM is enabled or disabled according to an optional input (On/off). The default value of this input is off.

These components integrate to perform some functions. Some of these functions are described in the following subsection.

5.2. *TPM functions*

A TPM runs a secure program which performs one or more of the following functions:

Digital signature. The most important concern of TPM is to ensure the authenticity of participants' contributions. A TPM uses the stored information required for authentication such as passwords, certificates and/or keys for signing the sensed data. This enables the data to be verified by the server. Additionally, a TPM can generate anonymous contributions by signing them with the private key (AIK) besides using some certificates which are granted by a trusted third party for verification. The TPM can thus help to preserve the participant's anonymity (e.g. [38,39]).

Hardware based cryptography. A TPM has the ability to encrypt the data before storing it into PCR. It uses the keys

[1] http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

generated by the key generator module and/or the AIK for data encryption. This mechanism is used to ensure that the data stored are protected from unauthorized software access. Therefore, this function makes it much harder to access the stored information without proper authorization (e.g. [95]).

Recording software run-time configuration. Although a TPM is a hardware solution for trust, it is not only concerned with the hardware that capture the sensed data, but also with the application software which carries out the local data processing on the participants' mobile devices. However, a TPM does not have the ability to control which software is launched on the participant's device. Nevertheless, it has the ability to store the run-time configurations of the software. Thus, a TPM can send these data along with the participant's contribution to the server. The server is then able to verify that only the authorized software configurations are adopted for data processing. If the reported configurations differ from the required ones, it means that the software has been attacked. Consequently, the received contributions will not be trusted by the server (e.g. [96]).

5.3. TPM goals

Through the functions described above, TPM can assure one or more from the following objectives:

- ***Attesting integrity***: Integrity attestation is the main goal of TPMs. This property assures the authenticity of participants' contributions. It confirms that the data received from a participant are indeed captured by authenticated sensor that resides on the participant's mobile device. Hence, it enables the application server to trust the reported data as authentic. This property is sometimes referred to as *remote attestation*. The signature function is the one which is responsible for the assurance of such goal (e.g. [38,39]).
- ***Data protection, sealed storage***: This property assures that the data are protected from unauthorized access. This implies that only authorized users and software can access these data. This goal can be assured through the incorporation of a hardware based cryptography function (e.g. [95]).
- ***Secure boot***: This property ensures that a mobile device can boot only the authorized trusted hardware and software configuration. This guarantees that the sensed data are processed only through the trusted hardware and software. The function of storing the software run-time configurations satisfies this goal (e.g. [96]).
- ***Participant privacy***: A sensing report usually contains personal and sensitive information about the participant. This information can be exploited for participant re-identification. Although, preserving participants' privacy is not a primary goal of TPM trust systems, in general, some TPM trust systems consider this issue in participatory sensing such as the systems presented in [95,96].

5.4. TPM merits and limitations

Most of existing trust systems (such as [38,39,95–97]) assure integrity attestation. Additionally, other systems can achieve the secure boot goal (such as [96]). While some TPM-based approaches are able to assure data protection and user anonymity (such as [95]).

We can deduce that TPM-based trust is considered as a viable solution for trust assessment in participatory sensing applications. However, the goals achieved by these systems do not imply that they can detect the existence of corrupted contributions. TPM seeks to assure integrity regardless participant's honesty. Dishonest participants create some interference to corrupt their contributions. Consequently, the need arises for trust systems which can measure the quality of contributions and estimate the honesty of participants. Therefore, reputation-based trust systems have been introduced seeking to satisfy these needs.

Furthermore, concerning TPM availability, TPM trust systems require smartphones or computing devices with special sensors that are manufactured to support trust systems through an embedded hardware chip. Thus, this property raises the prices of these devices that support TPM. Consequently, the devices with embedded TPM are currently not manufactured for the mainstream market. Moreover, there is no guarantee that all participants who join sensing campaigns are equipped with such devices. In addition, embedded chips consume more energy, computation, and communications capabilities, which may inhibit participants to join sensing campaigns.

These limitations obstruct the widespread use of TPM-based trust systems for the moment. To the best of our knowledge, TPM is still a mostly theoretical framework that has not been widely applied to real life participatory sensing. However, it has been successfully applied in other network domains such as [40].

6. Reputation systems

In the previous section, we have discussed TPM-based trust. It is evident that TPM is not a practical solution for trust assessment till the moment. Thus, researchers direct their efforts towards reputation-based trust assessment methods. Reputation is an aggregated opinion of the community members about how much an individual or an entity can be trusted. A person who needs to interact with a stranger, often considers his reputation to determine the amount of trust that he can place in him.

In recent years, reputation systems have gained popularity as a solution for securing distributed applications from misuse by dishonest entities. A reputation system computes the reputation scores of the entities in the system based on the feedback provided by fellow entities. A reputation system makes an entity accountable for its behavior by creating the possibility of losing good reputation and eventual exclusion by the community. Reputation systems make certain that users are able to gauge the trustworthiness of an entity based on the history of its behavior. The expectation that people will consider one another's pasts in future interactions constrains their behavior in the present [28,82].

As described before, in participatory sensing, participants behavior affect the quality of their provided contributions. Thus, reputation here is much more related to the quality of participant's contributions. Therefore, in the context of participatory sensing, Wang et al. [37] define the term reputation, as the synthesized probability that the past sensing reports sent by the participant is correct, as perceived by the server. Thus, in the context of participatory sensing, reputation-based trust systems do not consider only participants' related information such as the feedback of their followers, but they consider the quality of their provided contributions as well.

In the following subsection, we present how reputation is used to assess trust in participatory sensing applications.

6.1. Reputation-based trust system

Reputation-based trust systems usually have four main phases [57]: (1) information collection; (2) information mapping to trust score; (3) dissemination and (4) decision making.

Based on a comprehensive study of existing trust systems in participatory sensing, we have deduced a new framework of reputation-based trust systems. We depict this framework in Fig. 5. In this framework, we describe in details the first two phases of reputation-based trust system (i.e. (1) information collection, (2) information mapping to trust score). The highlighted parts of the figure define the different sources of information exploited in the information collection phase. While the rest of the figure parts describe how the available information is used to assess the trust of participants through the second phase (i.e. information mapping to trust score). In the following subsections, the details of this figure are discussed.

In a participatory sensing campaign, the server publishes a set of tasks that participants decide to join. When a given participant, participant P_i in the figure, captures his observations for a specific task $Task_j$, he constructs one or more sensing reports R_{P_i} for this task, and sends these reports to the application server. The server then gathers observations from different participants to carry out the required analysis. In addition, a trust system is applied to assess the trust of participants and their provided contributions as follows:

6.1.1. Information collection

Different information sources have been used to assess the trust of a participant. These sources include a watchdog module (*WDM*), users' feedback, community trust, and the history data of the target participant.

Watchdog module. WDM evaluates participant's current contribution (e.g., [92]). Sensing reports that belong to the same task are grouped together. Some consensus and outlier detection algorithms discussed in [98–100] are then used to evaluate the quality of a participant's contribution. These algorithms measure the similarity and consistency of each contribution compared with the other contributions provided by other participants. The higher the similarity of a contribution the more reliable it is. It is commonly assumed that the system is free of collusion or Sybil attacks. Otherwise, this measure can be biased. The result of a WDM is referred to as *Report Evaluation* (*RE*) (steps 1a, 1b, and 1c).

Users' feedback. Some reputation systems permit end users to assign some feedback to the provided contributions [86]. A user x may assign a feedback to a contribution R_{P_i} of participant P_i referred to as *Feedback* (F_x) (step 2).

Users should honestly share both positive and negative feedback. Indeed, sharing only positive or only negative feedback exposes trust systems to different types of attacks such as bad mouthing, and ballot stuffing attacks discussed in Section 3.1. Consequently, a feedback F_x should be evaluated. In Section 6.1.2, we explain how F_x is evaluated.

Community trust. A trust server may query his neighbors about their trust of the target participant. We refer to this type of information as the Community Trust *CT* as shown in the (step 3) of Fig. 5. The trust data provided by the community members should also be verified against different rating attacks, Section 6.1.2 discusses this step.

History. Another type of information is the old trust scores stored at trust databases. Old trust score of a participant P_i is noted as $OldT_{P_i}$ in the (step 4) of Fig. 5.

Following the different sources of information described above, we can deduce that the collected information is created either *manually* or *automatically*. On the one hand, manual information is usually created as an evaluation of a participant's current contribution (e.g., the output of WDM). On

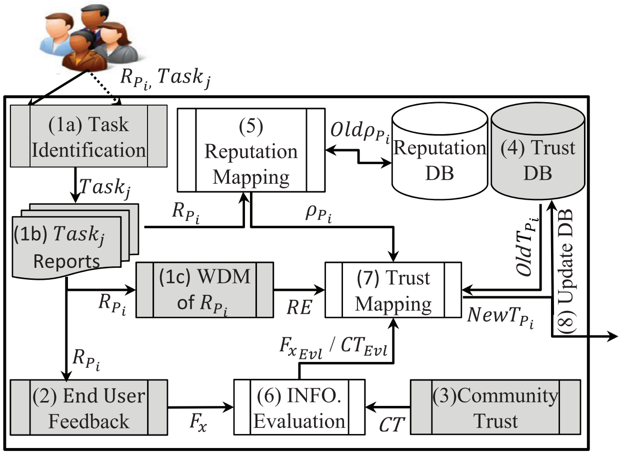


Fig. 5. A framework of reputation-based trust system.

the other hand, automatic information is an available trust data either stored at trust databases (i.e. direct information) or received as a feedback and responses to the trust queries (i.e. indirect information).

Thereafter, the collected information is used to assign a trust score to the participant through the trust mapping phase as shown in Fig. 5 (steps 5, 6, and 7). In the following section, we discuss the details of this phase.

6.1.2. Information mapping into trust score

The mapping process is carried out either in a centralized or a distributed way. In centralized mapping, participants' contributions and end users' ratings are exploited by a single entity in the trust system to calculate the new scores. This entity calculates a new reputation ρ_{P_i} and/or trust score $NewT_{P_i}$ for each participant, and updates the participants' record in the related database (e.g. [86]). Instead, in distributed mapping systems, the mapping process is distributed over more than one entity in the system. For example, in [89], both the end user and the server map a new reputation score for each participant.

Reputation mapping. In this phase, the first objective is to assign a new reputation score ρ_{P_i} to the participant. Here, a reputation mapping function is adopted (step 5). According to the literature [57], such reputation mapping function is either *deterministic* or *probabilistic*. In deterministic mapping, the output is computed according to a set of well-defined input values. Oppositely, probabilistic mapping functions have the possibility of an error (within some known bounds) and an unpredictable output due to some randomness in their input values. Various approaches have been applied to compute reputation scores of participants [27,101].

Due to the novelty of incorporation of trust management solutions into participatory sensing applications, not all the reputation computation methods that have been used in other domains have been investigated yet. Most of the current trust systems rely on either Bayesian reputation as a probabilistic approach [102] or the Gompertz function as a deterministic approach [103] for reputation mapping. The characteristics of these functions are very suitable for trust construction within participatory sensing environments. This is because the output of these functions dynamically reflects the changes in the participant's behavior along time. Thus, participants' behavior can be effectively traced using one of these functions. Additional characteristics are discussed as part of the definition of these function hereafter.

Bayesian model. Beta distribution is a statistical distribution which is defined according to the two parameters α and β. Its probability density function f for $0 \le x \le 1$ is formulated in Eq. (1) as follows:

$$f(x/\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} \times x^{(\alpha-1)} \times (1-x)^{(\beta-1)} \tag{1}$$

where, Γ is the gamma function, α and β represent the accumulated number of good and bad interactions of the participant respectively. The distribution domain is [0, 1]. The reputation is calculated by finding the expectation $E(\alpha, \beta)$ of the beta distribution according to Eq. (2).

$$\rho_{P_i} = E(\alpha, \beta) = \alpha/(\beta+\alpha). \tag{2}$$

An example of the Bayesian reputation plot is depicted in Fig. 6. The plot is generated for three participants with different behaviors. For instance, if the number of a participant's good interactions is significantly greater than the number of bad ones, the calculated reputation score usually exceeds 0.7. In Fig. 6, where $\alpha = 20$ and $\beta = 5$, the reputation score is 0.8. Oppositely, the calculated reputation score does not exceed 0.3 where the participant has more bad interactions than the good ones. Fig. 6 shows the case where $\alpha = 2$ and $\beta = 10$, the reputation score in this case is 0.16. Whereas, the participant is assigned a reputation score around 0.5 if the participant has a slight difference between his accumulated number of good and bad interactions. The example of $\alpha = 4$ and $\beta = 6$ reflects this case. The reputation score is 0.4. Hence, the reputation score calculated according to the expectation of the beta distribution reflects the type of behavior of the considered participant. Consequently, this model has the ability to measure the participant's deviation rate from the good behavior.

Furthermore, reputation should be calculated based on the most current information while keeping the effect of

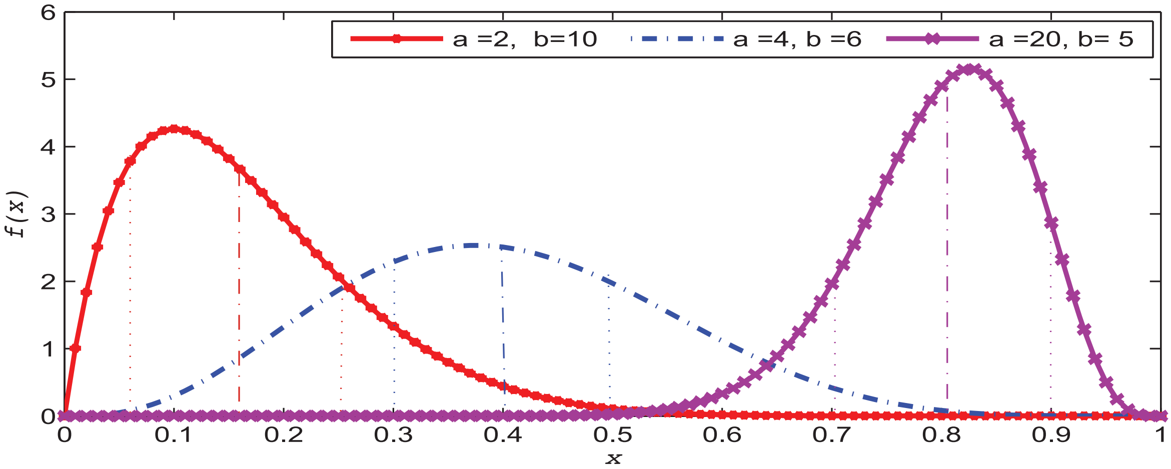


Fig. 6. The beta output of various types of participants.

some historical data. The Beta aging parameter w_{age} supports the ability to consider discounting of old information. The new values of α and β are calculated according to the following equations:

$$\alpha_{\text{new}} = w_{\text{age}} * \alpha_{\text{old}} + \alpha_{\text{current}} \tag{3}$$

$$\beta_{\text{new}} = w_{\text{age}} * \beta_{\text{old}} + \beta_{\text{current}}. \tag{4}$$

In this equation, w_{age} ranges from 1.0 which means keeping the entire history to 0.0 which means that no history was taken into consideration.

Gompertz function. Gompertz output gradually increases to reach its asymptote during a specific period of time. This behavior is reflective of trust construction in participatory sensing systems. For example, in such participatory sensing environments, trust is built gradually over a period of trustworthy behavior. It can also resemble some social parameters which positively affect trust such as friendship duration, the number of interactions between entities, etc. For example, long lasting relations are stronger than recent ones and subsequently are more trusted. Similarly, it is implied that the stronger the relation between entities, the higher the number of interactions between them during a given period of time. People are more interested to interact with persons with whom they are more familiar. These properties are well resembled by the output of Gompertz function. Gompertz is defined according to Eq. (5),

$$\rho_{P_i} = f(t) = a \times e^{-be^{-ct}}. \tag{5}$$

In this equation, a is the upper asymptote, b controls the displacement of the output along the x axis and c adjusts the growth rate of the function. The output of Gompertz belongs to the range [0, 1]. The output of Gompertz function for c = 1.5, 2.5, and 5 where b = 10 is depicted in Fig. 7(a).

As an example, consider t represents the number of interactions per day with the participant. We consider the Gompertz with $a = 1, b = 10, c = 1.5,$ in Fig. 7 (a). A participant who has 1 interaction per day is assigned a reputation score 0.11. Whereas, the participant with 3 interactions per day is assigned a reputation score 0.89.

Inverse Gompertz function. The output of inverse Gompertz function is used to resemble the parameters which negatively affect trust such as timeliness which represents the delay of participant responses. It is implied that, the more the delay of a participant respond to a task, the less concern he pays for it. Subsequently, late responses are usually assigned less trust scores and vice versa. Inverse Gompertz is defined in Eq. (6). The output of the inverse Gompertz function for different values of b is depicted in Fig. 7 (b),

$$\rho_{P_i} = f(t) = 1 - a \times e^{-be^{-ct}}. \tag{6}$$

As an example for the inverse Gompertz, consider t represents the timeliness of the participant's response in seconds. We consider the Gompertz with $a = 1, b = 20, c = 0.5,$ in Fig. 7 (b). A participant who has a timeliness of 1 s is assigned a reputation score 1. Whereas, the participant who has 10 s delay is assigned a reputation score 0.13.

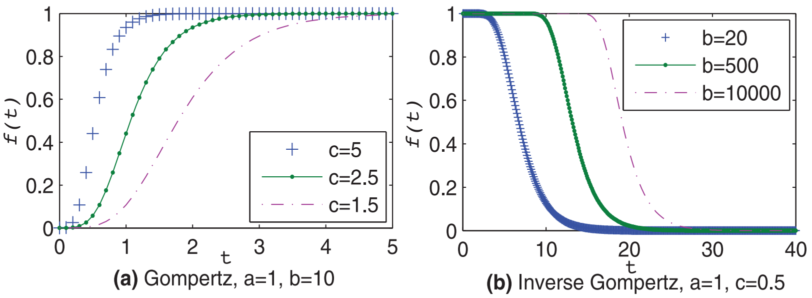
Both Gompertz and inverse Gompertz have the ability to integrate both some aging and reward/penalty mechanisms. For this, the input t is adjusted in order to reflect the aging parameter and reward/penalty mechanism as depicted in Eq. (7),

$$\acute{t} = \sum_{\acute{k}=1}^{k} \lambda^{(k-\acute{k})} \times t \tag{7}$$

where k is the total number of tasks which the participant joined, the summation is used to aggregate historical information. The impact of the old data is reduced through $\lambda^{(k-\acute{k})}$ with $0 \leq \lambda \leq 1$. λ is used as the aging parameter. It is referred to as aging weight. In addition, a reward/penalty mechanism can be adopted through replacing λ with two different values λ_s and λ_p. This implies two different rates for increasing or decreasing the reputation scores. λ_p is used with participants who have been witnessed to misbehave, such that $\lambda_p > \lambda_s$. This makes the reputation of a participant with λ_s increases more rapidly than the one with λ_p. Thus, misbehaved participant has to interact more cooperatively to neutralize the effect of his misbehavior.

Incorporating both aging parameter and reward/penalty mechanism gives the Gompertz function and its inverse better capabilities to reflect the features of the instantaneous behavior of participants. In addition, it deters participants to misbehave in order not to be penalized.

Information evaluation. The second objective of this phase is to verify the received information such as users feedback F_x and the trust scores received from the community CT against different rating attacks discussed in Section 3. Most trust systems in participatory sensing use the reputation ρ_x stored in the database of the rater x as a weight for his provided rating. Consequently, low weight is assigned to the rating provided by a user or entity with a poor reputation, and vice versa. The output of this module is referred to as Evaluated Feedback



(a) Gompertz, a=1, b=10

(b) Inverse Gompertz, a=1, c=0.5

Fig. 7. The output of Gompertz and Inv. Gompertz functions.

$F_{x\text{Evl}}$ and Evaluated Community Trust CT_{Evl} (step 6). However, this action does not solve the problem of different rating attacks; it only seeks to mitigate the effect of such attacks.

Trust mapping. The last issue, in this phase, is to assign a new trust level $NewT_{P_i}$ to participant P_i (step 7). Here, not only the current reputation score ρ_{P_i} is considered but also other parameters. These parameters include the current report evaluation *RE* evaluated by the WDM, the old trust level assigned to the participant $OldT_{P_i}$, the trust provided by the community CT_{Evl} and/or the users' feedback about the participant $F_{x\text{Evl}}$. Each trust system selects one or more of these parameters and aggregates them to calculate a new trust $NewT_{P_i}$ score of the participant. Finally, this new score is used to update the participant's record in the related databases (step 8).

6.1.3. Dissemination

This phase is realized either in a centralized or a distributed manner. In centralized dissemination, the reputation scores are stored in and propagated from a single entity. Additionally, the regularity of the dissemination process comes in one of two forms; *proactive* and *reactive* dissemination. In the proactive mode, the dissemination is performed periodically at a fixed rate. In the reactive mode, the dissemination is performed according to some triggers, events or when some threshold is reached. In other systems, a query message is required for obtaining trust scores [90].

6.1.4. Decision making

The final phase in reputation-based trust systems is the decision making. The decision mainly depends on the trust score assigned to the participant. Trust scores are either *discrete* or *continuous* values. Discrete trust scores use a set of discrete qualitative values such as (Very Untrustworthy, Untrustworthy, Trustworthy, Very Trustworthy). Continuous trust scores come in a range of values such as [0, 1]. If the trust score for a participant is greater than a predefined threshold, the participant's contribution is accepted. Moreover, the participant is then rewarded if the trust system applies an incentive/reward mechanism. Oppositely, if the trust score is below the threshold, the participant's contribution may be rejected and the participant may be penalized (if a penalty mechanism is adopted). This type of decision is referred to as a binary decision. However, some systems are designed to accept all received contributions. In these systems, the current trust score of the participant is used as a weight for his contribution. We called this type of decision as fusion.

In Fig. 8, the reputation-based trust systems' phases, functions and parameters described in the previous subsections are summarized.

In the following subsection, we define the goals that can be assured through reputation-based trust systems.

6.2. Properties of reputation-based trust systems

According to the previous discussion of reputation-based trust systems, one can identify the main properties of these systems as follows:

- ***Traceability***: It is more probable for the participant who used to be honest to have a good behavior in the future. Similarly, a participant who previously behaved maliciously is expected to provide untrusted contributions. Thus, participant's past behavior should reflect his current reputation and trust score.
- ***Freshness***: The reputation score assigned to a participant should increase or decrease to demonstrate the most recent trustworthiness qualities of this participant, as a function of his latest interactions.
- ***Separability***: Participants should not have control on the update process of their reputation scores. They should not have the ability either to maliciously interfere to update their scores or to demonstrate a forged or erroneous reputation score.
- ***Exposure***: Malicious participants should be exposed. Having committed a malicious behavior, participant should be identified as malicious and potentially evicted or at minimum his malicious contributions should be excluded. This property is referred to as *accountability*.

Anonymous reputation systems are vital for the success of participatory sensing as we discussed in Section 4.3. Anonymous reputation-based trust systems seek to achieve the previous goals while maintaining the anonymity of the participants' identity. The anonymity of a participant can be preserved by the satisfaction of the following goals as well. Some of these properties have been previously mentioned in [68].

- ***Anonymous login***: A participant should have the ability to login and to submit his reports anonymously. Participants' real identities should not be revealed.
- ***Non-associative***: A sensing report should include neither the participant's real identity nor a reference to his real identity. Hence, the server will not be able to relate the sensing report to a specific participant by anyway.
- ***MSR unlinkabelity***: The server should not have the ability to link multiple sensing reports (*MSR*) from the same participant.
- ***Anonymous demonstration***: Participants should have the ability to demonstrate their reputation scores to the server without revealing their real identities.

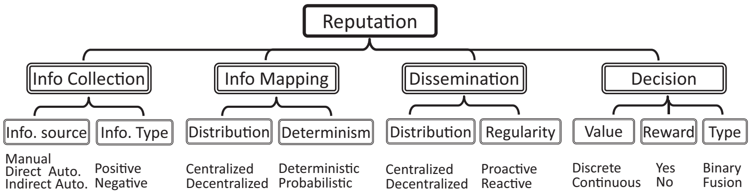


Fig. 8. Mapping trust in reputation-based trust system.

Both the satisfaction of these goals and the resistance against the previously mentioned attacks mainly depend on the strength of the trust system.

6.3. Merits and limitations of reputation-based trust

Most reputation-based trust systems (such as [68,85–89,92]) assure these goals (e.g. traceability, exposure, freshness, etc.). However, each trust system assures each one of these goals with different degrees of satisfaction. For instance, reputation trust systems have the ability to detect participants' misbehavior (i.e. exposure property). However, the speed to detect such misbehavior depends on the strength of the reputation mapping function. A reputation mapping function may incorporate some aging parameters to assign a higher weight to participants' recent interactions. Furthermore, reward and penalty rules can be applied (Section 6.1.2).

Most of the current trust systems use either Bayesian or Gompertz function for reputation mapping (Section 6.1.2). It was clear that the systems which exploit Gompertz mapping function have stronger capabilities than the other mapping functions exploited in participatory sensing. This is because Gompertz function has the ability to integrate both the aging parameters and the reward/penalty mechanisms, which enable the system to rapidly reflect new features of a participant's behavior on the assigned trust score. The systems that adopt the Gompertz function include [84–86,89]. While Bayesian model is exploited in [104,105].

In addition, some reputation-based trust systems are designed such that it can preserve the privacy of participants through the assurance of the goals of anonymous reputation system described above such [68,87–89]. These systems encourage participants to log-in sensing campaign without the fear of the possible privacy breaches.

In the next section, we present the state-of-the-art trust systems in participatory sensing applications.

7. Examples of trust systems from state-of-the-art

In the following, we describe different examples from the literature of trust management in participatory sensing. We classify these systems according to their distribution as described in Section 4.2.

7.1. Centralized trust systems

Centralized trust systems are those systems where trust scores of participants are maintained and stored by a trusted central third party. In the following, we discuss examples of these systems.

Manzoor et al., in [83,106], seek to compute the trustworthiness of participants' predictions about bus arrival times in a bus watch participatory sensing application. The trust server adopts a WDM to measure the deviation of the participant's prediction compared with others' predictions. This measure is fed into a Gaussian membership function to define the quality of each contribution. The output of the Gaussian function is combined with the old trust of the participant to estimate the instantaneous trustworthiness of this participant.

A centralized trust framework for social participatory sensing systems is introduced by Amintoosi et al. in [85]. This framework estimates a score of the *trust of contribution* (*ToC*). This score assesses both the *quality of contribution* (*QoC*) and the *trustworthiness of participant* (*ToP*). Some methods are adopted through a WDM to evaluate *QoC* (e.g. [99,100]). In addition, *ToP* is used to measure both the participants' capabilities and the strength of their relation with the requester (e.g. expertise, timeliness, locality, friendship duration, and interaction time gap). The system adopts both Gompertz and Inverse Gompertz to measure *ToP*. To calculate a *TOC* score of the participant, the system combines both of the *QoC* and the *ToP* via a fuzzy inference system [85].

The authors introduced an improved version of the previous system in [86,107]. A reputation and a subjective rating module are incorporated. The reputation module utilizes the *PageRank* algorithm [108] to calculate and update the reputation scores of participants. This algorithm relies on the difference between the number of nodes that trust the participant compared with the total number of his relations, the most trusted participants are assigned higher reputation scores. In addition, the subjective evaluation enables the requester to assign a rate to the participant's contribution as a user feedback. The reputation score of the requester is used as a weight for his provided rating. The new trust score of a participant is calculated based on the requester rating and *ToC* calculated according to the old version of this system [86,107]. Misbehaved participants are penalized by decreasing their trust scores. This system has the ability to trace and detect the participant's behavior through the continuous update of the reputation scores. It also reflects the change of the participant's behavior. Additionally, early detection and penalty of misbehaved participants act as a deterrent for malicious behavior.

Amintoosi et al. in [109], proposed another improved version of the system presented in [86,107] and discussed above. The authors propose a methodology to select the most appropriate and trustworthy participants among friends and friends of friends in a social participatory sensing network to attend sensing campaigns. First, the selection process depends on the compatibility between both the task requirements' parameters and participants' attributes. Participants who achieve an acceptable level of homogeneity with the task requirements are selected to attend the campaign. The most trusted paths to those participants are defined. In such social sensing network, routes from a requester to the selected participants can include other intermediate nodes. Thus, a depth first search is applied to define the most trusted route to those participants. The trust score of a route is calculated as a combination of the trust scores of each pair of nodes along the route. Then, the route with the highest trust score is selected. Moreover, a suggestion component is incorporated to build the list of participants who achieve a satisfactory behavior during multiple campaigns. Thus, it enables the requester to recruit the most appropriate participants to join the sensing campaign.

A privacy preserving reputation system for participatory sensing is presented by Huang et al. in [89]. The authors try to compromise between both participants' anonymity and the trust of their contributions. Participants share their contributions anonymously using some changeable pseudonyms.

The system relies on a trusted server referred to as (*TTP*). The server maintains a mapping list between participants' real identities and their associated pseudonyms. The server then assigns new reputation scores to the participants relying on Gompertz function described in Section 6.1.2. Hereafter, the server updates the corresponding reputation score and attaches it to the real identity. The server transfers the reputation score from the real identity to the next chosen pseudonym.

Gisdakis et al. introduced SPPEAR as a privacy preserving framework that assures both privacy of participants and accountability [87]. A group manager (*GM*) announces a list of tasks. A participant selects one or more and authenticates with the GM to obtain a private key and an authorization token from the GM. The participant shares this token with an *identity provider* (*IdP*) entity which provides participants with pseudonyms from a *Pseudonyms Certification Authority* (*PCA*). SPPEAR adopts a protocol for the revocation of participants who submit samples that deviate from the rest of the contributions. A resolution authority (*RA*) provides the pseudonyms of those participants to PCA, PCA provides RA an authorization token including an assertion that used to generate these pseudonyms. RA forwards this token to the IdP who blacklists all tokens of those pseudonyms and sends a confirmation to GM. A similar protocol is adopted for the revocation of participants who have malfunctioning devices and thus unintentionally provide some corrupted contributions.

Chang et al., in [67], propose a trust system for detecting Sybil attacks. Sybil nodes usually use the same radio channel for communication. Thus, this scheme detects the existence of Sybil nodes through defining the normal rates of some statistical measures of a participatory sensing network of interest (e.g. the number of participants who join the system campaigns at specific time). To determine if the node is genuine or Sybil, a regular check for these measures is performed by a *characteristics checking scheme* (*CCS*). Additionally, a *trust credit assessment* (*TCA*) module is adopted to collect the feedback reported about the nodes in the system. If both CCS and TCA find the measured rates outbound the normal ranges, the requester is notified that Sybil nodes may exist. Otherwise, the requester is notified that the network is free of such nodes. Although this system mainly depends on the CCS, it is considered as a reputation-based trust system because it aggregates the feedback of the nodes from the requesters which is a reputation mechanism.

7.2. Collaborative trust systems

In collaborative trust systems, each node in the system maintains and stores trust scores in its own storage, as defined in Section 4.2.

LotS is a privacy preserving reputation framework that is presented by Michalas et al. in [88]. In this framework, a participant joins one of the groups created previously by a *registration authority* (RA). Participants can anonymously share their contributions with another entity *C* by signing them with the group signature. If the contribution is verified to be correct, the recipient forward it to the rest of the community. Each community member can send a voting request to *C* to evaluate the contribution received. *C* should make sure that each entity has the ability to send no more than one voting request for the same sensing report. These votes are then aggregated to calculate a reputation score of the concerned participant.

Yang et al. presented a system in [91] that enables the campaign administrator to filter out untrusted participants. First, the system exploits participant's reputation derived from both the quality of their current contribution and their old reputation scores. Feedback scores derived from the community members are aggregated. Moreover, some personal information about the participant is integrated. Each one of these parameters is assigned a score. According to the scores of these parameters, a weighted sum trust score is calculated for each participant. Participants are then ranked based on these trust scores. Finally, the most trusted participants are selected to attend the campaign. Although the authors presented an integrated framework for trust assessment, they only define the system parameters that should be considered. They do not go through how these parameters should be measured.

Kalidindi et al., in [90], exploited both personal and community opinions to evaluate the trustworthiness of a specific participant. First, each contribution is assigned either positive or negative feedback by the requester. This feedback is determined by calculating the numerical scores of some parameters such as the response time, time gap, familiarity, reciprocity, and the relevance parameters. Gompertz and inverse Gompertz are used for these scores. Subsequently, the score of each contribution is calculated as a weighted sum of these parameters' scores. If the score of a contribution exceeds a certain threshold, the contribution is assigned a positive feedback and vice versa. In general, the responding node is assigned a positive opinion if the number of its positive contributions exceeds a specific threshold. The requester then queries the community opinion about the responding node. Finally, both personal and community opinions are integrated to evaluate the trust score of each node.

7.3. Hybrid trust systems

As previously discussed in Section 4.2, we refer to a trust system as a hybrid system when the application server manages both the application campaigns and participants' trust as well. These systems are constructed as either reputation or TPM-based systems. Here, hybrid reputation-based trust systems are presented, followed by hybrid TPM-based trust ones.

7.3.1. Hybrid reputation-based trust systems

In [104], Reddy et al. proposed a set of metrics that enable for evaluating the participants' contributions. Participants who have some experience in the current task are selected to join the campaign. Additionally, a contribution is defined to be successful if it is captured by the appropriate sensor at the required time and location. This system adopts Bayesian reputation function described in Section 6.1.2.

Reddy et al. in [105] proposed a recruitment framework to define the most trusted participants for a campaign. This system depends on the participant's reputation while the Bayesian model is used to compute this reputation score as explained in Section 6.1.2. Non-cooperative participants are defined by measuring the probability that a participant is going to contribute his observation when it is available, or not. The system seeks to measure the quality and quantity of samples that are expected from a participant. In this system, Bayesian model was used for reputation estimation.

In [84,92], Huang et al. proposed a system for evaluating the trustworthiness of participants' contributions in noise monitoring participatory sensing applications. Each device is assigned a reputation score, which depends on the quality of the reports submitted by this device in a specific period of time. Reports which belong to the same sensing location are grouped and directed to a watchdog module (WDM). WDM produces a set of ratings in the range [0, 1]. The rating of each contribution is used as a weighting coefficient to minimize the impact of corrupted ones. It also acts as input to a subsequent reputation module. The system incorporates some historical information about the device. Moreover, it adopts the reward/penalty mechanism. The reputation module computes a reputation score based on Gompertz function. The experimental results indicate that this system quickly adapts the reputation scores, according to the changes of participants' behavior.

Wang et al. in [37,68] proposed a privacy preserving reputation system. In the registration phase, the server grants the participant two reputation certificates (i.e. the first including participant ID while the second does not include this ID). The first certificate is used to construct one or more blinded ID [110] to submit one or more sensing report anonymously. The second certificate is involved in the sensing report. The system allows participants to cloak their time and location data. It then calculates sensitivity parameters to define contributions that are captured outside the required sensing area and time. In addition, a similarity factor is evaluated to measure the consistency of a participant's report with other reports of the same task (WDM). The server assesses the trust of a participant based on the reputation score contained in the certificate beside the sensitivity parameters and the similarity measure. The participant is assigned a positive feedback if the final trust score exceeds the current trust score contained in the reputation certificate, and vice versa.

This system maintains both the data trust and the participant's anonymity. Therefore, the participant ID and the sensing report cannot be correlated. Additionally, multiple reports which sent from the same participant cannot be linked to each other. Moreover, both negative and positive reputation updates are enforced. However, a large number of participants is required to preserve the participant's anonymity. Otherwise, the participant's identity can be compromised.

Restuccia et al. introduced a framework (FIDES) in [36] to defend against the GPS spoofing attacks. A mobile security agent (MSA) is deployed into the sensing area (e.g. a taxi driver). The application guarantees the reliability of the reports provided by the MSA due to some reward or additional credits which provided to this agent. The application asks both participants and MSA to share their sensed data. Participant's contribution is used to update his reputation score. FIDES adopts the trust model proposed in [111] to model the uncertainty about participants reputation. In addition, this score is used to judge the contribution and to calculate the reward that should be assigned to this participant. Depending on MSA, to define the normal behavior of participants, makes this framework robust against different types of attacks such as corruption, discrimination, reputation lag, assuming that MSA will not abuse.

Kazemi et al. try to assure both the trust of participants' contributions and their privacy preservation in TAPAS [112]. The system allows multiple participants to collect their observations at each data collection point (*DC*-point) redundantly. The contribution that achieves the majority consensus is verified as correct. Consequently, the larger number of the participant at the DC-point, the more the chance that the collected data are correct. The system assigns DC-points to the participants based on a privacy preserving technique [113]. Therefore, participants cannot be compromised to a location based attack.

7.3.2. Hybrid TPM-based trust systems

A trusted platform based framework for participatory sensing is introduced by Dua et al. in [39]. An application running on a participant's phone is responsible for taking integrity measurements and passing them to TPM. The application server sends an attestation request to verify the trustworthiness of a participant's contribution. In this case, TPM signs the recorded integrity measurements and sends them to the server. The contribution is considered trustworthy if it is correctly verified with the measurements received from the TPM.

In [38], authors try to attest the integrity of sensed data through supporting each sensor with TPM referred to as *angel*. The role of the angel is to execute a code signed by a trusted third party. This code attests the integrity of the sensed data through signing it. TPM is supported by a hardware cryptographic module. The private key is burned into the chip. Additionally, data are encrypted to achieve data protection. This system is resistant to both collusion and Sybil attacks. Furthermore, it ensures both content protection and access control mechanism using a broadcast encryption technique. However, uploading raw sensed data is highly expensive for mobile devices. Moreover, contributing data in their raw form acts as a deterrent to participants to contribute their personal information.

Both trust of a participant's contribution and privacy preservation are considered by Gilbert et al. in [96]. First, TPM launches a trusted software to carry out the required local processing on the raw sensed data. The data are recorded into PCR concatenated with their hash value. PCR content is updated only using the hash value of the current PCR (*extend operation*). Additionally, TPM signs its PCR in order to attest the software used for report generation. Furthermore, TPM has the ability to encrypt the data and bind them with a specific software. Consequently, only trusted software is able to access the data storage. On the application server side, the hardware used is verified using the certificate issued by a certificate authority provider. The application server compares PCR contained in the report with the expected values to assess the software validation. This system shares the same advantage and limitations of the system presented in [38] and discussed above. Additionally, a trusted software is used for local data processing.

The idea presented by Saroiu et al. in [95] is to integrate TPM functionality with each individual sensor reading. Each sensor reading is signed by the sensor from which it was captured. In addition, a small trusted code in the cloud is used to verify the raw sensor reading and to combine these readings. Subsequently, a registration process is used by the service cloud to link between the sensors and the device in which it resides.

In [97], Gilbert et al. adopted an analyzer for evaluating the participants' contributions. This analyzer has the ability to measure the differences between the data that are shared by a participant and the original sensor reading. Thus, this system assures the data authenticity. However, the authors adopt a TPM emulator as a building block instead of TPM hardware.

8. General analysis and comparisons

In this section, we use different frameworks introduced in Sections 4–6 to make comparisons between the various trust systems that have been presented in the literature and discussed in Section 7. We used these comparisons to discuss all existing trust systems and conclude them in the field of participatory sensing.

8.1. General comparison

In Table 2, different trust systems are compared according to the proposed classification framework. For more details, about the nature of each of the classification's dimensions, the merits and limitations of each of them, please refer to Section 4. The comparison defines the distribution, the methodology adopted by each trust system and whether the system is anonymous or non-anonymous. Table 2, columns of distribution, methodology, and anonymity depict this comparison.

8.1.1. Analysis of TPM trust

According to the TPM goals described in Section 5.3, Table 2 shows the guarantees that can be assured by each one of the TPM trust systems. Most of these systems (such as [38,39,95–97]) assure integrity attestation. Additionally, other systems can achieve the secure boot goal (such as [96]). Whereas, some TPM-based systems are able to assure data protection (such as [96]), and user anonymity (such as [95]).

TPM has the ability to achieve a high level of security and integrity through the assurance of the previous goals. However, these systems suffer from many limitations. One of these limitations is that they cannot detect misbehaved participants. In addition, devices equipped with TPM are not usually available with participants who join the sensing campaigns. For more details about the merits and limitations of TPMs refer to Section 5.4. In general, TPM solutions have some merits. However, they still have some obstacles to be applied to a real life participatory sensing system.

8.1.2. Analysis of reputation-based trust

The goals of reputation-based trust system have been discussed in Section 6.2 (e.g. traceability, exposure, freshness, etc). Most reputation-based trust systems (such as [68,85–89,92]) assure these goals as depicted in Table 2. However, the strength of the reputation system and its speed for detecting misbehaved participants depend on the system parameters and the exploited mapping function (Section 6.1.2).

Table 2
Comparison of the trust systems in terms of the analysis framework.

System	Distribution	Methodology	Anonymity	Characteristics										
				TPM			Reputation				Anonymity			
				Attestation	Data protec.	Secure boot	Traceability	Freshness	Separability	Exposure	Anon. login	Non-associative	MSR Unlinked	A non demon.
Dua et al. [39]	Hybrid	TPM	N-anon	√	–	–	–	–	–	–	–	–	–	-
Dua et al. [38]	Hybrid	TPM	N-anon	√	√	–	–	–	–	–	–	–	–	-
Gilbert et al. [96]	Hybrid	TPM	Anon	√	√	√	–	–	–	–	–	–	–	-
Saroiu et al. [95]	Hybrid	TPM	Anon	√	–	–	–	–	–	–	√	–	–	-
Gilbert et al. [97]	Hybrid	TPM	N-anon	√	–	–	–	–	–	–	–	–	–	-
Reddy et al. [104]	Hybrid	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Reddy et al. [105]	Hybrid	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Yang et al. [91]	Coll.	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Huang et al. [84,92]	Hybrid	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Jkalidindi et al. [90]	Coll.	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Manzoor et al. [83]	Cen	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Amintoosi et al. [85]	Cen	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Amintoosi et al. [86,107]	Cen	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Amintoosi et al. [109]	Cen	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Chang et al. [67]	Cen	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Wang et al. [37,68]	Hybrid	Rep	Anon	–	–	–	√	√	√	√	√	√	√	√
Huang et al. [89]	Cen	Rep	Anon	–	–	–	√	√	√	√	√	√	–	√
Restuccia et.al. [36]	Cen	Rep	N-anon	–	–	–	√	√	–	√	–	–	–	-
Michalas et.al. [88]	Coll	Rep	Anon	–	–	–	√	√	√	√	√	√	√	√
Gisdakis et.al. [87]	Cen	Rep	Anon	–	–	–	√	√	–	√	√	√	√	-
Anon	Anonymoys	**Cen**		Centralized				**Coll**			Collaborative			
N-anon	Non anonymous	**Rep**		Reputation				√, –			Goal satisfied or not			

Table 3
Analysis of the trust systems in terms of robustness to attacks.

System/attack	Corr	Onof	Ree	Dis	Col	Syb	Lag	GPS	Unf	Bad	Ball
Dua et al. [39]	*	–	***	–	***	***	–	–	–	–	–
Dua et al. [38]	*	–	***	–	***	***	–	–	–	–	–
Gilbert et al. [96]	*	–	***	–	***	***	–	–	–	–	–
Saroiu et al. [95]	*	–	***	–	***	***	–	–	–	–	–
Gilbert et al. [97]	*	–	***	–	***	***	–	–	–	–	–
Reddy et al. [104]	*	*	–	–	–	–	**	–	–	–	–
Reddy et al. [105]	*	*	–	–	–	–	**	–	–	–	–
Yang et al. [91]	–	–	–	–	–	–	*	–	**	–	–
Huang et al. [84,92]	*	**	–	–	–	–	***	*	–	–	–
Jkalidindi et al. [90]	–	–	–	–	–	–	*	–	**	–	–
Manzoor et al. [83]	**	**	–	–	–	–	**	*	–	–	–
Amintoosi et al. [85]	**	*	–	–	–	–	***	*	**	–	–
Amintoosi et al. [86,107]	***	**	–	–	–	–	***	*	**	–	–
Amintoosi et al. [109]	***	***	–	–	–	–	***	*	**	–	–
Chang et al. [67]	–	–	–	–	–	***	*	–	*	–	–
Wang et al. [37,68]	**	**	**	–	–	**	**	*	***	–	–
Huang et al. [89]	**	**	**	–	–	**	**	–	***	–	–
Restuccia et al. [36]	***	***	**	–	***	**	*	***	*	–	–
Michalas et al. [88]	*	–	**	–	–	**	*	–	*	–	–
Gisdakis et al. [87]	**	–	**	–	–	**	*	*	*	–	–
* Weak	** Semi Robust				*** Robust				– Attack not addressed		
Bad badmouthing	Ball	Ballot stuffing	Col	Collusion	Cor	Corruption		GPS	GPS spoofing	Lag	Reputation lag
Onof on-off	Ree	Re-entry	Syb	Sybil	Unf	Unfair rating		–	–	–	–

In general, reputation-based trust systems which adopt Gompertz function as a reputation mapping function offer strong capabilities for tracing and detecting misbehaved participants [86,92,109]. This is because Gompertz function has the ability to integrate both the aging parameters and the reward/penalty mechanisms, which enable the system to rapidly reflect new features of a participant's behavior on the assigned trust score.

8.1.3. Privacy preserving reputation systems

The goals of privacy preserving reputation system have been discussed in Section 6.2. These goals include anonymous login, non-associative, and anonymous demonstration. The systems presented in [68,87–89] have the ability to preserve participant's anonymity (Table 2). These systems satisfy the goals of privacy preserving reputation systems. These reputation systems give more chances for participatory systems to be more successful. While participants are motivated to log-in sensing campaigns if they make sure that the systems provide them with strong privacy guarantees.

The reputation systems which we have presented in [114,115] do not hide the identity of participants but preserve the confidentiality of their feedback. Such reputation systems are suitable for environments where participant anonymity is not possible or feedback confidentiality is the main privacy goal.

8.1.4. Comparison based on distribution

As mentioned before, in Section 4.2, in participatory sensing, trust systems have three different distributions: centralized, collaborative, and hybrid. Each one has its own characteristics as discussed before. Some instances of centralized trust systems are presented in [85–87,89]. While, [88,90,91] are collaborative systems, and [36,37,92] are hybrid trust systems. The merits, as well as the limitations of each of those distributions, are discussed in 4.2.1.

To sum up, each one of the possible distributions has some advantages and disadvantages. Thus, designers of participatory systems can select the distribution of the trust system which suits the considered participatory system.

8.2. Analysis of attack robustness

Participatory sensing systems are vulnerable to various attacks as described in Section 3.1. Each of the proposed trust systems shows different degrees of resistance against each of those attacks. Table 3 summarizes this comparison. In the following, we discuss the resistance of TPM trust systems to different types of attacks followed by that of reputation-based trust systems.

8.2.1. Robustness of TPM trust systems

It is evident that most of TPM-based trust systems are robust against re-entry, Sybil and on-off attacks [38,95–97]. TPM trust systems assure the authenticity of participants' contributions. Thus, the application server can make sure that the participant's contribution has been captured by an authentic sensor. Therefore, participants have to use another device to launch such attacks, this inhibits attacks of these types.

TPM assures the secure boot property, which implies that the appropriate hardware configuration is used to capture the observations. It also ensures that only trusted software is used for local processing of these observations. Hence, participants have minimum control on their own observations. Consequently, they have little opportunity to coordinate their behaviors to achieve some malicious goals (i.e. collusion attack). Subsequently, TPM systems are resistant under collusion attack.

Although, these systems are robust against these previous attacks, they are considered weak against corruption attacks. TPM cannot detect malicious participants who deliberately initiate sensing actions to corrupt their observations, as discussed before in Section 3.1. Additionally, the other attacks are not considered with TPM trust systems.

8.2.2. Robustness of reputation-based trust systems

Regarding reputation-based trust systems, we can note that the trust scores usually depend on one or more of the following parameters:

- The participant's old trust or reputation score.
- The quality of the current contribution.
- The end users' feedback about the contribution.
- The neighbors' rating of the participant.

Each reputation-based trust system selects one or more of the previous parameters and adopts a specific reputation mapping function to calculate a trust score for every participant. Therefore, each system has a different degree of resistance against various attacks. From the discussion of the state-of-the-art of existing trust systems in participatory sensing presented in Section 7, we can deduce the following:

Corruption attack. The system presented in [36] is considered robust against corruption attack. This system depends on a mobile secure agent which provides the system with the most accurate information. Thus, the system can accurately define corrupted contributions.

Other trust systems depend on double checking way to define the quality of a contribution. First, outlier detection or consensus algorithms [98–100] are used to measure the deviation of the contribution from a common consensus. Second, users are permitted to assign a feedback to a participant based on their satisfaction with the received contribution. Trust systems that adopt both the first and the second measures are considered robust against this attack [86,109]. Systems that adopt only one of these measures are semi-robust against this attack [37,83,87,92]. However, the systems that only depend on the past interactions of the participant as a measure of trust weakly defend against this attack (such as [104,105]), because participants may instantaneously change their behavior.

Reputation lag exploitation attack. The reputation mapping function should apply more aggressive penalties concerning misbehaved participants. This allows a trust system to have an up to date trust scores which reflect the instantaneous trustworthiness of each participant. Thus, misbehaved participants have a minimum opportunity to exploit the reputation lag for injecting corrupted or forged contributions into the system. Gompertz function applies more strong penalties compared with the other mapping functions. Therefore, trust systems that depend on the Gompertz function are more rapidly adaptive for reflecting changes in the participants' behavior. Consequently, Gompertz based trust systems are robust against reputation lag exploitation attack (such as [84–86,109]).

Bayesian based reputation trust systems (such as [68,83,104,105]) are considered semi-robust against this attack. The reputation systems presented in [67,90] are weak against the reputation lag exploitation attack, because both of them only depend on the community opinions and feedback about the participant and they have no way to penalize misbehaved participants.

On-off attack. On-off attacker alternates between normal and abnormal behavior. Thus, the way to defend against this attack is to have a good capabilities to monitor and trace participants' behavior. In addition, the system should involve a mechanism to evaluate the quality of the participants' contributions to be more resistant to this attack. Thus, systems which satisfy both these guarantees are robust against on-off attack. These methods include [36,68,83,86,92,109]. However, semi-robust trust systems (such as [85,89]) only assure either the first or the second guarantee. The reputation trust systems that neglect the quality of contribution are considered weak against this attack. The systems presented in [67,104,105] are considered as examples of such systems.

Collusion attack. Collusive participants are supposed to coordinate their behaviors to achieve some malicious goals. However, trust systems adopt different algorithms that rely on consensus to measure the consistency of the participants' contributions compared with the contributions of other participants for the same task. These algorithms comprise of consensus algorithms [84], similarity measures [68], deviation from common values [83], or outlier detection algorithms [85,86,109]. These methods fail to properly evaluate the contributions while collusion is committed. Trust systems can provide resistance to collusion given that the number of well-behaved participants is larger than the number of collusive ones. Therefore, most trust systems are considered to defend weakly against collusion attack except [36] which is considered robust. This system compares the contributions with the one which received from a secure agent. Thus, it is resistant to collusion attack.

Sybil attack. Sybil attack can be launched if a participant has the ability to obtain different identification parameters. In [67], the authors address the Sybil attack. They try to analyze the system statistically in order to detect the existence of a Sybil nodes. Thus, this system is considered robust against this attack. Furthermore, the Sybil attack was mentioned by the authors in [68]. The authors suggest that the participants commit some limited resource while logging into the system. However, this solution is considered weak for such an attack. In addition, we consider trust systems which adopt some authentication mechanism as semi-robust to defend against this attack [36,37,87–89], since participants still have the ability to obtain different identities unless a strong authentication technique is applied. The rest of existing systems do not address this attack.

Re-entry attack. A re-entry attack occurs when a participant with a low reputation score leaves the system and rejoins using different identification parameters. Therefore, the attacker has the ability to avoid the consequences of his misbehavior. The resistance of different systems to defend against such attack depends on the attacker ability to obtain different authentication parameters. Thus, systems have the same resistance towards re-entry attack as their resistance towards Sybil attack. The systems presented in [36,37,87–89] are semi-robust to defend against such attack. However, the system presented by Chang et al. [67] is robust against Sybil attack. It cannot defend against re-entry attack since this system depends on a statistical analysis of the number of

Table 4
Comparison of reputation-based trust systems.

System	Information collection				Mapping		Dissemination		Decision		
	Source	Type	WDM	Attack	Structure	Approach	Structure	Approach	Value	Type	Reward/penalize
Reddy et al. [104]	M/D	+,–	N	G	Cen	Pr	–	–	Cont	B	N
Reddy et al. [105]	D	+,–	N	G	Cen	Pr	–	–	Cont	B	N
Yang et al. [91]	D/I/M	+,–	Y	G	–	–	–	–	Disc	B	N
Huang et al. [84,92]	M/D	–	Y	Corr	Cen	De	–	–	Cont	F	Y
Jkalidindi et al. [90]	M/D/I	+,–	N	G	Cen	De	Dis	Re	Cont	B	N
Manzoor et al. [83]	M/D	–	Y	Corr	Cen	Pr	–	–	Cont	F	N
Amintoosi et al. [85]	M	–	N	G	Cen	De	Cen	–	Cont	B	N
Amintoosi et al. [86,107]	M/I	+,–	N	G	Cen	De	Cen	–	Cont	B	Y
Amintoosi et al. [109]	M/I	+,–	N	G	Cen	De	Cen	–	Cont	B	Y
Chang et al. [67]	M/I	+,–	N	Sybil	Cen	–	Cen	Re	Cont	B	N
Wang et al. [37,68]	M/D	–	Y	G	Cen	De	–	–	Disc	B	N
Huang et al. [89]	D	+,–	Y	G	Cen	De	–	–	Cont	B	N
Restuccia et al. [36]	M/D	–	Y	GPS	Cen	De	–	–	Disc	B	Y
Michalas et al. [88]	I	–	N	G	Cen	–	–	–	–	B	N
Gisdakis et al. [87]	M	–	Y	G	Cen	–	–	–	–	B	N
- Not mentioned	**B**	Binary			**Cen**	Centralized			**Cont**	Continuous	
Corr corruption attack	**D**	Automatic direct			**De**	Deterministic			**Dis**	Distributed	
Disc discrete	**F**	Fusion			**G**	General misbehavior			**GPS**	GPS spoofing	
I automatic indirect	**M**	Manual			**N**	No			**Pr**	Probablistis	
Re reactive	**Y**	Yes			–	–			–	–	

participants joining the system at a point in time. This can detect the participant who synchronizes different identities to login the system. While re-entry attacker completely leave the system and login again using a new identity.

GPS spoofing attack. The system presented in [36] is considered robust against this attack. Depending on a trusted mobile secure agent, enables the system to define the most accurate sensed data in the sensing area. Thus, the system can easily define dishonest participants who share inconsistent information with the sensing area. Existing trust systems that can assess the quality of participant's contribution weakly defend against this type of attack [85,86,92,109]. Additionally, trust systems that do not consider the quality of participant's contribution cannot defend against this attack.

Unfair rating attack. Most of the current reputation-based trust systems for participatory sensing is considered weak against the unfair rating attack. Some systems allow participants to share their contributions anonymously so that a rater has no motivation to commit unfair rating against an anonymous participant. One of the trust systems that defend against unfair ratings attack through anonymity preservation is presented in [68]. Some other systems try to overcome unfair rating attack by trying to mitigate its effect. Since the participants with high reputation scores are more likely to be honest, these systems use the reputation score of the rater as a weight for the rate which he submits. These systems (e.g., [86,90,109]) are thus considered semi-robust against the unfair rating attack. The systems (such as [67]) that adopt the rating methodology without consideration for the degree of honesty of the rater are weak against this attack.

Others. Bad mouthing, ballot stuffing, and discrimination attacks are not addressed by any of existing trust systems in participatory sensing.

8.3. *Comparison of reputation-based trust systems*

A comparison of the reputation-based trust systems is shown in Table 4. This table indicates how each phase in the reputation-based trust system is implemented according to the framework illustrated in Section 6.1 and summarized in Fig. 8. We focus on the particularities which characterize the implementation of each of existing trust system individually.

9. Future research directions

Trust systems have been a focus of research for a number of years in various application domains. However, trust management in the context of participatory sensing systems is still an area where research is in its infancy. There are a number of open issues that need to be resolved. First, the devices of participants usually have limited resource capabilities. Second, according to our study, many trust goals have not been satisfied yet. Third, many types of attacks have not been treated. Additionally, each of the current trust systems treats only a few of the many issues which should be considered in such environments. In this section, we highlight the unsolved research challenges of trust systems for participatory sensing.

1. *Attacks:*
   In Section 3.1, we discussed the possible attacks in participatory sensing. The resistance of existing trust systems under each one of the addressed attack is discussed in Section 8.2. From this study, we can conclude that many types of attacks have not been addressed yet. These include discrimination, re-entry, bad mouthing, and ballot stuffing attacks. Moreover, the defense mechanisms for some other types of attacks, such as Sybil and unfair rating, are still in their infancy. We can also observe that most reputation systems are mainly concerned with detecting malicious participants who commit corruption attacks that may disrupt the application server. However,

much less attention has been directed toward other types of attacks.

2. *Privacy:*
   Trust systems in participatory sensing applications seek to identify malicious participants who contribute corrupted, fabricated, or erroneous contribution. Malicious participants should be discarded during the task assignment phase and their contributions should be excluded through the campaign. These goals conflict with the objectives of preserving the privacy and anonymity of the participants. This issue was considered by privacy preserving reputation-based trust systems as presented in [37,88,89,112,116]. Most of these systems depend on the group signature [117], anonymization [118], and blind signature [110] to preserve the identity of participant. However, there are other techniques applied on literature for privacy preservation within a reputation systems such as anonymous credential systems [119], Zero knowledge proof [120]. It is clear that the compromise between the conflicting goals of both trust assessment and privacy preservation still needs a lot of work to be assured.
3. *Reputation mapping:*
   As we described in Section 6.1.2, existing reputation-based systems adopt either Gompertz function [103] or Bayesian model [102] as a reputation mapping functions. Although Gompertz function offers better capabilities for tracing participants' behavior more than Bayesian model, both of these functions still do not assure the guarantees of a robust and reliable trust assessment system. Different mapping functions were used in the literature of trust [121]. However, various other reputation mapping function can be adopted which may better fit with participatory sensing such as gamma or Weibull distribution model [122].
4. *User and environment centricity:*
   As mentioned in [24] and explained in Section 2, participatory sensing applications may be either personal centric or environment centric. In personal centric applications, sensitive information about a participant is transferred to the application server, which may then give feedback, advice, or new sensing commands to the participant. In this case, the participant needs to ensure the trustworthiness of the application server in order to share his sensitive information. However, in environment centric applications, contributions are captured from the surrounding environment and forwarded to the application server. The server uses these contributions for analyzing or mapping some phenomena. In contrast, this scenario makes it important for the application server to assess the trustworthiness of participants. Hence, a trust system should ideally manage the trust for both these types of applications. To the best of our knowledge, existing trust systems focus on trust from the environment centric applications point of view. These systems target to assess the trust of participants. While assessing the trustworthiness of application server should target to confirm that the application server will not grant access of the participant's personal information to any untrusted third party. This problem has not been addressed by any of the current systems.
5. *Ensuring the trustworthiness of different parties:*
   As mentioned in [41] and discussed in Section 2, different parties need to be considered in participatory sensing campaign (e.g. participant, campaign administrator, and users). Each party has his own capabilities and concerns which differ according to the application. In addition, each one has the ability to tamper with the sensing campaign. Accurately assessing the trustworthiness of all parties is vital for the normal functioning of participatory sensing campaigns.
6. *Measuring the quality of contributions:*
   In participatory sensing, trust systems usually adopt some consensus or outlier detection algorithms such as [98,99]. These methods have the ability to measure the deviation of a contribution from a common consensus. However, the quality estimation is biased if the majority of participants are malicious or if a collusion is committed. Therefore, measuring the quality of the participants' contributions is one of the challenges that face trust systems in participatory sensing applications.
7. *Resource overhead:*
   Applying trust systems requires loading the system entities with additional overhead. This overhead may be additional battery consumption or computational power. This overhead is often critical for the different parties in the system, especially the participants who are usually equipped with smartphones or other computational devices with limited capabilities. Most trust systems in participatory sensing domain have not discussed this issue. Therefore, further research should be directed toward studying and reducing the resource overhead of trust systems.
8. *Scalability:*
   In participatory sensing systems, a large number of contributions is required to enable the system to carry out a stable measurement and analysis for the phenomenon under consideration. Thus, a large number of participants is usually required in sensing campaigns. Moreover, numerous message exchanges are required by each participant to accomplish a sensing campaign. Therefore, the performance of these systems may degrade due to the addition of more participants to the system. Consequently, management of trust and reputation for large-scale participatory sensing systems is an issue that should be addressed by future work.

10. Related work

Trust management has been studied extensively in various domains of distributed computing.

In wireless sensor networks, sensor nodes may share corrupted data due to damage or malfunctioning sensor or problems in the communication between the node and the sink node. Therefore, monitoring the behavior of nodes is essential in order to detect any deviation from the normal nodes' behavior. Researchers investigated this issue [33][34][35]. Both wireless sensor networks and participatory sensing share a set of attacks that can be launched in both these environments. However, Here, a different framework of trust system is exploited which fits the nature of participatory sensing. In addition, there are some special guarantees that should be fulfilled within participatory sensing environment.

In peer to peer systems, the network is established from several distributed peers with equal privilege. Those peers should share the available resources as well as the workload. Peers are allowed to join and leave the system at any time. P2P systems do not include a central management unit that should assure the security and trust issues among the peers. Thus, P2P systems are vulnerable to malicious peer behaviors which addressed in different surveys such as [29]. These systems face a different set of attacks. In addition, the reputation framework adopted in peer to peer network is completely different from the one adopted in participatory sensing.

Mobile ad-hoc networks are structureless and dynamic networks. These networks consist of mobile nodes that have no fixed link between them. These networks have a dynamic topology and no stable structure. Users can join and leave the network within a random period of time affecting the energy, bandwidth, and memory computations of the network. Managing trust in these networks is a crucial task because many activities such as routing rely heavily on the cooperation and trustworthiness of the users. Many researchers survey how trust can be assessed in mobile ad-hoc networks such as [30–32].

Trust should be maintained also in online applications (e.g. E-commerce) to encourage the buyers to perform transactions with the sellers. The trust score assigned to a seller enables the buyer to estimate the trustworthiness of the provided service. In [121], Jaøsang studies how to assess trust within online applications. This work addresses different models for reputation mapping in trust systems. However, trust systems in participatory sensing mainly adopt different models such as Gompertz mapping and Bayesian model as we discussed in our survey.

Mobile social networks are a specific type of social networks that seek to merge the merits of both social networks and opportunistic networks. Users, in mobile social network, are able to share and access user-centric data using their mobile devices. Najaflou et al. [123] define the trust-related and other attacks faced by these systems and study the state of the art in this domain. It was clear that the attacks faced by participatory sensing differ from the ones that faced by such mobile social networks.

Trust also has been studied in other different domains such as in opportunistic networks [124–126]. Trust management is a promising area of research which attracts researchers' interest in different domains. Here, we have just mentioned some examples of such works. To sum up, studying trust in participatory sensing has its own features and particularities which we seek to cover in our analysis.

11. Conclusion

Participatory sensing systems are an emerging type of systems that seek to achieve welfare in different areas of human life. Applications of participatory sensing systems enable humans to save time (e.g., by sensing traffic), improve their health (e.g., by monitoring their health status), and live richer lives (e.g., by documenting their daily activities), etc. These systems exploit the mobile devices of regular citizens for capturing and sharing their sensed data. However, involving regular citizens in the sensing campaigns exposes these systems to some challenges. The main challenge is the uncertainty of the participants behaviors because different attacks can be launched from misbehaved participants. Consequently, trust systems have been proposed to detect the misbehaved participants and/or at least to mitigate the effect of their misbehavior.

In this paper, trust assurance among stakeholders in participatory sensing systems is addressed. We proposed a classification framework of these systems. It is observed that the current trust systems can be classified mainly into TPM-based and reputation-based systems. We provided in-depth analysis of each type of these systems. We conclude that TPM is not sufficient as a stand-alone solution for trust assessment in such environment. Nevertheless, reputation systems can provide more guarantees toward participants' accountability. Such reputation-based trust systems incorporate various measures for assessing the trust of participants. These measures include a WDM to measure the quality of contribution, the users' feedback, the community opinion, and the historical information concerning the target participant. However, the decisions of reputation systems may be biased because of different attacks.

Furthermore, we presented a general analysis and comparisons of the existing trust systems and discussed their resistance against the addressed attacks. It is evident that reputation systems which adopt the Gompertz function as a reputation mapping function are more robust against the addressed attacks. In addition, such systems provide more strong capabilities for tracing the participants' behavior instantaneously.

Finally, we identified many trust problems that have not been solved and many attacks have not been addressed yet in the literature. From these, we list the open challenges that need to be addressed by future work on trust systems in participatory sensing. One of the major challenges of reputation systems in participatory sensing is managing the accountability of participants while preserving their privacy. Participants are vulnerable to some security breaches such as identity leakage since reputation systems have to manage the linkability of participants' contributions with their real identities in order to manage their trust. Another major challenge is how the trust systems can evaluate the participant's contribution. Existing system adopt some consensus and outlier algorithms that can be biased in the existence of some attacks. Different limitations and more open challenges are discussed within this paper. We hope this work helps to elucidate the current state-of-the-art of this domain for researchers as well as system designers.

References

[1] Cisco, its affiliates, Cisco visual networking index: global mobile data traffic forecast update 2013 2018, Technical report, 2014.

[2] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M.B. Srivastava, Participatory sensing, in: Workshop on World-Sensor-Web (WSW 06): Mobile Device Centric Sensor Networks and Applications, 2006, pp. 117–134.

[3] N.D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, A.T. Campbell, A survey of mobile phone sensing, IEEE Commun. Mag. 48 (9) (2010) 140–150.

[4] M. Annavaram, N. Medvidovic, U. Mitra, S. Narayanan, G. Sukhatme, Z. Meng, S. Qiu, R. Kumar, G. Thatte, D. Spruijt-Metz, Multimodal sensing for pediatric obesity applications, in: Proceedings of the International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense), 2008, pp. 21–25.

[5] T. Denning, A.H. Andrew, R. Chaudhri, C. Hartung, J. Lester, G. Borriello, G. Duncan, Balance: towards a usable pervasive wellness application with accurate activity inference, in: HotMobile, 2009.

[6] E. Kanjo, J. Bacon, D. Roberts, P. Landshoff, Mobsens: making smart phones smarter, IEEE Perv. Comput. 8 (4) (2009) 50–57.

[7] L. Nachman, A. Baxi, S. Bhattacharya, V. Darera, N. Kodalapura, V. Mageshkumar, S. Rath, R. Acharya, Jog falls: a pervasive healthcare platform for diabetes management, in: Pervasive Computing, 6030, 2010, pp. 94–111.

[8] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, Peir, the personal environmental impact report, as a platform for participatory sensing systems research, in: MobiSys09, Krakw, Poland, 2009.

[9] P. Mohan, V.N. Padmanabhan, R. Ramjee, Nericell: rich monitoring of road and traffic conditions using mobile smartphones, in: Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems, in: SenSys '08, ACM, New York, NY, USA, 2008, pp. 323–336.

[10] R.K. Ganti, N. Pham, H. Ahmadi, S. Nangia, T.F. Abdelzaher, Greengps: a participatory sensing fuel-efficient maps application, in: Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, in: MobiSys '10, ACM, New York, NY, USA, 2010, pp. 151–164.

[11] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A.M. Bayen, M. Annavaram, Q. Jacobson, Virtual trip lines for distributed privacy-preserving traffic monitoring, in: Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services, in: MobiSys '08, ACM, New York, NY, USA, 2008, pp. 15–28.

[12] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, J. Eriksson, Vtrack: accurate, energy-aware road traffic delay estimation using mobile phones, in: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, in: SenSys '09, ACM, New York, NY, USA, 2009, pp. 85–98.

[13] N. Maisonneuve, M. Stevens, B. Ochab, Participatory noise pollution monitoring using mobile phones, Inform. Polity 15 (1,2) (2010) 51–71.

[14] R.K. Rana, C.T. Chou, S.S. Kanhere, N. Bulusu, W. Hu, Ear-phone: an end-to-end participatory urban noise mapping system, in: Proceeding of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN10), Stockholm, Sweden, 2010, pp. 105–116.

[15] E. Paulos, R. Honicky, E. Goodman, Sensing atmosphere, in: SenSys 2007, Sydney, Australia, 2007.

[16] E.A. Garcia, R.F. Brena, Real time activity recognition using a cell phone's accelerometer Wi-Fi., in: Intelligent Environments (Workshops), in: Ambient Intelligence and Smart Environments, 13, IOS Press, 2012, pp. 94–103.

[17] T. Choudhury, G. Borriello, S. Consolvo, D. Haehnel, B. Harrison, B. Hemingway, J. Hightower, P.P. Klasnja, K. Koscher, A. LaMarca, J.A. Landay, L. LeGrand, J. Lester, A. Rahimi, A. Rea, D. Wyatt, The mobile sensing platform: an embedded activity recognition system, IEEE Perv. Comput. 7 (2) (2008) 32–41.

[18] G.-S. Ahn, M. Musolesi, H. Lu, R. Olfati-Saber, A.T. Campbell, Metrotrack: predictive tracking of mobile events using mobile phones, in: Proceedings of the 6th IEEE International Conference on Distributed Computing in Sensor Systems, in: DCOSS'10, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 230–243.

[19] S. Consolvo, D.W. McDonald, T. Toscos, M.Y. Chen, J. Froehlich, B. Harrison, P. Klasnja, A. LaMarca, L. LeGrand, R. Libby, I. Smith, J.A. Landay, Activity sensing in the wild: a field trial of UbiFit garden, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, in: CHI '08, ACM, New York, NY, USA, 2008, pp. 1797–1806.

[20] N. Györbíró, A. Fábián, G. Hományi, An activity recognition system for mobile phones, Mobile Netw. Appl. 14 (1) (2009) 82–91.

[21] Y.F. Dong, S. Kanhere, C.T. Chou, N. Bulusu, Automatic collection of fuel prices from a network of mobile cameras, in: Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor Systems, in: DCOSS '08, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 140–156.

[22] L. Deng, L.P. Cox, Livecompare: grocery bargain hunting through participatory sensing, in: Proceedings of the 10th Workshop on Mobile Computing Systems and Applications, in: HotMobile '09, ACM, New York, NY, USA, 2009, p. 4.

[23] K. Shilton, Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection, Commun. ACM 52 (11) (2009) 48–53.

[24] W. Khan, Y. Xiang, M. Aalsalem, Q. Arshad, Mobile phone sensing systems: a survey, Commun. Surv. Tutorials, IEEE 15 (1) (2013) 402–427.

[25] A. Kapadia, D. Kotz, N. Triandopoulos, Opportunistic sensing: security challenges for the new paradigm, in: Proceedings of the First International Conference on COMmunication Systems And NETworks, in: COMSNETS'09, IEEE Press, Piscataway, NJ, USA, 2009, pp. 127–136.

[26] D. Christin, Privacy in mobile participatory sensing: current trends and future challenges, J. Syst. Softw. (2015), doi:10.1016/j.jss.2015.03.067.

[27] A. Jøsang, Trust and reputation systems, in: FOSAD, 2007, pp. 209–245.

[28] P. Resnick, K. Kuwabara, R. Zeckhauser, E. Friedman, Reputation systems, Commun. ACM 43 (12) (2000) 45–48.

[29] C. Selvaraj, S. Anand, A survey on security issues of reputation management systems for peer-to-peer networks, Comput. Sci. Rev. 6 (4) (2012) 145–160.

[30] Y.S. Renu Dalal, Manju Khari, Survey of trust schemes on ad-hoc network, in: Advances in Computer Science and Information Technology. Networks and Communications, Part 1, in: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 84, second international conference, CCSIT 2012, Bangalore, india, January 2—4, 2012. Proceedings, Part I, Springer Berlin Heidelberg, 2012.

[31] J.-H. Cho, A. Swami, I.-R. Chen, A survey on trust management for mobile ad hoc networks, IEEE Commun. Surv. Tutorials 13 (4) (2011) 562–583.

[32] K. Ramana, A.A. Chari, N. Kasiviswanth, A survey on trust management for mobile ad hoc networks, in: International Journal of Network Security & Its Applications, 2, 2, April 2010, p. 75.

[33] O. Khalid, S.U. Khan, S.A. Madani, K. Hayat, M.I. Khan, N. Min-Allah, J. Kolodziej, L. Wang, S. Zeadally, D. Chen, Comparative study of trust and reputation systems for wireless sensor networks, Secur. Commun. Netw. 6 (6) (2013) 669–688.

[34] H. Alzaid, M. Alfaraj, S. Ries, A. Jøsang, M. Albabtain, A. Abuhaimed, Reputation-based trust systems for wireless sensor networks: a comprehensive review, in: IFIPTM, 2013, pp. 66–82.

[35] M.C.F. Gago, F. Martinelli, S. Pearson, I. Agudo (Eds.), Trust Management VII - 7th IFIP WG 11.11 International Conference, IFIPTM 2013, Malaga, Spain, June 3-7, 2013. Proceedings, IFIP Advances in Information and Communication Technology, 401, Springer, 2013.

[36] F. Restuccia, S.K. Das, Fides: A trust-based framework for secure user incentivization in participatory sensing, in: A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on, IEEE, 2014, pp. 1–10.

[37] X.O. Wang, W. Cheng, P. Mohapatra, T. Abdelzaher, Enabling reputation and trust in privacy-preserving mobile sensing, IEEE Trans. Mobile Comput. 99 (PrePrints) (2014) 1.

[38] A. Dua, N. Bulusu, W.-C. Feng, W. Hu, Towards trustworthy participatory sensing, in: Proceedings of the 4th USENIX Conference on Hot Topics in Security, in: HotSec'09, USENIX Association, Berkeley, CA, USA, 2009, p. 8.

[39] A. Dua, W. Hu, N. Bulusu, Demo abstract: a trusted platform based framework for participatory sensing, in: Proceedings of the 2009 International Conference on Information Processing in Sensor Networks, in: IPSN '09, IEEE Computer Society, Washington, DC, USA, 2009, pp. 419–420.

[40] T.C. Group, Trusted platform modules strengthen user and platform authenticity, 2005. URL: http://www.trustedcomputinggroup.org/files/resource_files/8D46621F-1D09-3519-ADB205692DBBE135/Whitepaper_TPMs_Strengthen_User_and_Platform_Authenticity_Final_1_0.pdf.

[41] D. Christin, A. Reinhardt, S.S. Kanhere, M. Hollick, A survey on privacy in mobile participatory sensing applications, J. Syst. Softw. 84 (11) (2011) 1928–1946.

[42] D.C. Brabham, Crowdsourcing as a model for problem solving an introduction and cases, Convergence: Int. J. Res. New Media Technol. 14 (1) (2008) 75–90.

[43] J. Howe, The rise of crowdsourcing, wired, june 2006, Information on: http://www.wired.com/wired/archive/14.06/crowds.html (2011).

[44] R.K. Ganti, F. Ye, H. Lei, Mobile crowdsensing: current state and future challenges, IEEE Commun. Mag. 49 (11) (2011) 32–39.

[45] E. Kanjo, Noisespy: a real-time mobile phone platform for urban noise monitoring and mapping, Mobile Netw. Appl. 15 (4) (2010) 562–574.

[46] A. Thiagarajan, J. Biagioni, T. Gerlich, J. Eriksson, Cooperative transit tracking using smart-phones, in: Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems, in: SenSys '10, ACM, New York, NY, USA, 2010, pp. 85–98.

[47] Waze application. URL https://www.waze.com/.

[48] S. Reddy, A. Parker, J. Hyman, J. Burke, D. Estrin, M. Hansen, Image browsing, processing, and clustering for participatory sensing: lessons from a dietsense prototype, in: Proceedings of the 4th Workshop on Embedded Networked Sensors, in: EmNets '07, ACM, New York, NY, USA, 2007, pp. 13–17.

[49] E.P. Stuntebeck, J.S. Davis II, G.D. Abowd, M. Blount, Healthsense: classification of health-related sensor data through user-assisted machine learning, in: Proceedings of the 9th Workshop on Mobile Computing Systems and Applications, in: HotMobile '08, ACM, New York, NY, USA, 2008, pp. 1–5.

[50] J.R. Kwapisz, G.M. Weiss, S.A. Moore, Activity recognition using cell phone accelerometers, SIGKDD Explor. Newsl. 12 (2) (2011) 74–82.

[51] S.B. Eisenman, E. Miluzzo, N.D. Lane, R.A. Peterson, G.-S. Ahn, A.T. Campbell, The BikeNet mobile sensing system for cyclist experience mapping, in: Proceedings of the 5th International Conference on Embedded Networked Sensor Systems, in: SenSys '07, ACM, New York, NY, USA, 2007, pp. 87–101.

[52] S.B. Eisenman, E. Miluzzo, N.D. Lane, R.A. Peterson, G.-S. Ahn, A.T. Campbell, Bikenet: a mobile sensing system for cyclist experience mapping, ACM Trans. Sens. Netw. (TOSN) 6 (1) (2010) 6:1–6:39.

[53] T.A. Charu C. Aggarwal, Managing and Mining Sensor Data, Social Sensing, Springer US, 2013.

[54] T. Dimitrakos, R. Moona, D. Patel, D.H. McKnight (Eds.), Trust Management VI - 6th IFIP WG 11.11 International Conference, IFIPTM 2012, Surat, India, May 21-25, 2012. Proceedings, IFIP Advances in Information and Communication Technology, 374, Springer, 2012.

[55] K. Kifayat, M. Merabti, Q. Shi, D. Llewellyn-Jones, Security in Wireless Sensor Networks , Handbook of Information and Communication Security, Springer Berlin Heidelberg, 2010.

[56] A. Jøsang, J. Golbeck, Challenges for robust of trust and reputation systems, in: Proceeding of the 5th International Workshop on Security and Trust Management (STM 2009), 2009.

[57] K.J. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Comput. Surv. (CSUR) 42 (1) (2009).

[58] L.F. Perrone, S.C. Nelson, A study of on-off attack models for wireless ad hoc networks, in: First IEEE International Workshop on Operator-Assisted (Wireless Mesh) Community Networks (OpComm 2006), Berlin, Germany, 2006.

[59] Y. Chae, L. Cingiser Dipippo, Y.L. Sun, Trust management for defending on-off attacks, IEEE Transactions on Parallel and Distributed Systems 26 (4) (2015) 1178–1191.

[60] H. Alzaid, E. Foo, J.G. Nieto, E. Ahmed, Mitigating on-off attacks in reputation-based secure data aggregation for wireless sensor networks, Secur. Commun. Netw. 5 (2) (2012) 125–144.

[61] S. Abbas, M. Merabti, D. Llewellyn-Jones, Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks, in: Wireless Days (WD), 2010 IFIP, 2010, pp. 1–6.

[62] M. Feldman, C. Papadimitriou, J. Chuang, I. Stoica, Free-riding and whitewashing in peer-to-peer systems, IEEE J. Select. Areas Commun. 24 (5) (2006) 1010–1019.

[63] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, A. Oliveira, Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation, Springer, 2011.

[64] J.M. Hernández-Muñoz, J.B. Vercher, L. Muñoz, J.A. Galache, M. Presser, L.A.H. Gómez, J. Pettersson, Smart Cities at the Forefront of the Future Internet, Springer, 2011.

[65] H. Chourabi, T. Nam, S. Walker, J.R. Gil-Garcia, S. Mellouli, K. Nahon, T.A. Pardo, H.J. Scholl, Understanding smart cities: an integrative framework, in: System Science (HICSS), 2012 45th Hawaii International Conference on, IEEE, 2012, pp. 2289–2297.

[66] C. Marforio, A. Francillon, S. Capkun, S. Capkun, S. Capkun, Application collusion attack on the permission-based security model and its implications for modern smartphone systems, Department of Computer Science, ETH Zurich, 2011.

[67] S.-H. Chang, Y.-S. Chen, S.-M. Cheng, Detection of Sybil attacks in participatory sensing using cloud based trust management system, in: Wireless and Pervasive Computing (ISWPC), 2013 International Symposium on, 2013, pp. 1–6.

[68] X.O. Wang, W. Cheng, P. Mohapatra, T.F. Abdelzaher, Artsense: anonymous reputation and trust in participatory sensing., in: INFOCOM, IEEE, 2013, pp. 2517–2525.

[69] W. Wei, F. Xu, C. Tan, Q. Li, Sybildefender: defend against sybil attacks in large social networks, in: INFOCOM, 2012 Proceedings IEEE, 2012, pp. 1951–1959.

[70] A. Mohaisen, N. Hopper, Y. Kim, Keep your friends close: incorporating trust into social network-based sybil defenses, in: INFOCOM, 2011 Proceedings IEEE, 2011, pp. 1943–1951.

[71] D. Quercia, S. Hailes, Sybil attacks against mobile users: friends and foes to the rescue, in: INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1–5.

[72] H. Yu, M. Kaminsky, P. Gibbons, A. Flaxman, Sybilguard: defending against Sybil attacks via social networks, IEEE/ACM Trans. Netw. 16 (3) (2008) 576–589.

[73] W. Premchaiswadi, W. Romsaiyud, N. Premchaiswadi, Navigation without GPS: fake location for mobile phone tracking, in: 11th International Conference on ITS Telecommunications (ITST), 2011, 2011, pp. 195–200.

[74] A. Jhumka, M. Bradbury, M. Leeke, Fake source-based source location privacy in wireless sensor networks, Concur. Comput. Pract. Exper. 27 (2015) 2999–3020, doi:10.1002/cpe.3242.

[75] L. Zhang, S. Jiang, J. Zhang, W.K. Ng, Robustness of trust models and combinations for handling unfair ratings, in: Trust Management VI, Springer, 2012, pp. 36–51.

[76] Y.-F. Yang, Q.-Y. Feng, Y.L. Sun, Y.-F. Dai, Dishonest behaviors in online rating systems: cyber competition, attack models, and attack generator, J. Comput. Sci. Technol. 24 (5) (2009) 855–867.

[77] A.A. Irissappane, S. Jiang, J. Zhang, Towards a comprehensive testbed to evaluate the robustness of reputation systems against unfair rating attack., in: UMAP Workshops, 12, 2012.

[78] T. Dimitrakos, R. Moona, D. Patel, D.H. McKnight, Trust management VI: 6th IFIP WG 11.11 International Conference, IFIPTM 2012, Surat, India, May 21-25, 2012, Proceedings, Springer Publishing Company, Incorporated, 2012.

[79] Z. Banković, J.C. Vallejo, D. Fraga, J.M. Moya, Detecting bad-mouthing attacks on reputation systems using self-organizing maps, in: Proceedings of the 4th International Conference on Computational Intelligence in Security for Information Systems, in: CISIS'11, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 9–16.

[80] Y.L. Sun, Z. Han, W. Yu, K.R. Liu, Attacks on trust evaluation in distributed networks, in: Information Sciences and Systems, 2006 40th Annual Conference on, IEEE, 2006, pp. 1461–1466.

[81] V. Cortier, J. Detrey, P. Gaudry, F. Sur, E. Thome, M. Turuani, P. Zimmermann, Ballot stuffing in a postal voting system, in: Requirements Engineering for Electronic Voting Systems (REVOTE), 2011 International Workshop on, 2011, pp. 27–36.

[82] O. Hasan, Privacy preserving reputation systems for decentralized environments, INSA de Lyon, 2010 Thse de doctorat en informatique.

[83] A. Manzoor, M. Asplund, M. Bouroche, S. Clarke, V. Cahill, Trust evaluation for participatory sensing, in: MobiQuitous, 2012, pp. 176–187.

[84] K.L. Huang, S.S. Kanhere, W. Hu, Are you contributing trustworthy data?: the case for a reputation system in participatory sensing, in: Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, in: MSWIM '10, ACM, New York, NY, USA, 2010, pp. 14–22.

[85] H. Amintoosi, S.S. Kanhere, A trust framework for social participatory sensing systems, in: MobiQuitous, 2012, pp. 237–249.

[86] H. Amintoosi, S.S. Kanhere, A reputation framework for social participatory sensing systems, MONET 19 (1) (2014) 88–100.

[87] S. Gisdakis, T. Giannetsos, P. Papadimitratos, Sppear: security & privacy-preserving architecture for participatory-sensing applications, in: Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks, ACM, 2014, pp. 39–50.

[88] A. Michalas, N. Komninos, The lord of the sense: a privacy preserving reputation system for participatory sensing applications, in: Computers and Communication (ISCC), 2014 IEEE Symposium on, IEEE, 2014, pp. 1–6.

[89] K.L. Huang, S.S. Kanhere, W. Hu, A privacy-preserving reputation system for participatory sensing, in: Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks (LCN 2012), in: LCN '12, IEEE Computer Society, Washington, DC, USA, 2012, pp. 10–18.

[90] R.R. Kalidindi, K.V.S.V.N. Raju, V.V. Kumari, C.S. Reddy, Trust based participant driven privacy control in participatory sensing, CoRR abs/1103.4727 (2011).

[91] P.R. HaoFan Yang Jinglan Zhang, Using reputation management in participatory sensing for data classification, in: Procedia Computer Science, The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT-2011) / The 8th International Conference on Mobile Web Information Systems (MobiWIS 2011), 5, 2011, pp. 190–197.

[92] K.L. Huang, S.S. Kanhere, W. Hu, On the need for a reputation system in mobile phone based sensing, Ad Hoc Netw. 12 (2014) 130–149.

[93] T.C. Group, Tpm main specification. URL http://www.trustedcomputinggroup.org/resources/.

[94] T.C. Group, Trusted platform module (tpm) summary (2008). URL: https://www.trustedcomputinggroup.org/news/Industry_Data/TPM_applications_paper_March_28_2008.pdf.

[95] S. Saroiu, A. Wolman, I am a sensor, and I approve this message, in: Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, in: HotMobile '10, ACM, New York, NY, USA, 2010, pp. 37–42.

[96] P. Gilbert, L.P. Cox, J. Jung, D. Wetherall, Toward trustworthy mobile sensing, in: Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, in: HotMobile '10, ACM, New York, NY, USA, 2010, pp. 31–36.

[97] P. Gilbert, J. Jung, K. Lee, H. Qin, D. Sharkey, A. Sheth, L.P. Cox, Youprove: authenticity and fidelity in mobile sensing, in: SenSys, 2011, pp. 176–189.

[98] M.M. Breunig, H.-P. Kriegel, R.T. Ng, J. Sander, Lof: identifying density-based local outliers, SIGMOD Rec. 29 (2) (2000) 93–104.

[99] S. Papadimitriou, H. Kitagawa, P. Gibbons, C. Faloutsos, Loci: fast outlier detection using the local correlation integral, in: 19th International Conference on Data Engineering, 2003. Proceedings., 2003, pp. 315–326.

[100] S. Reddy, A. Parker, J. Hyman, J. Burke, D. Estrin, M. Hansen, Image browsing, processing, and clustering for participatory sensing: lessons from a dietsense prototype, in: in EmNets 07: Proceedings of the 4th Workshop on Embedded Networked Sensors, ACM Press, 2007, pp. 13–17.

[101] A. Aldini, R. Gorrieri (Eds.), Foundations of security analysis and design IV, FOSAD 2006/2007 Tutorial Lectures, Lecture Notes in Computer Science, 4677, Springer, 2007.

[102] A. Jøsang, R. Ismail, The beta reputation system, in: In Proceedings of the 15th Bled Electronic Commerce Conference, 2002.

[103] F.J. Kenney, K.S. E., Mathematics of Statistics, in: Part 1, third, Princeton, NJ: Van Nostrand, 1962.

[104] S. Reddy, K. Shilton, J. Burke, D. Estrin, M. Hansen, M. Srivastava, Evaluating participation and performance in participatory sensing, in: Proceedings of the International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense08), 2008.

[105] S. Reddy, D. Estrin, M. Srivastava, Recruitment framework for participatory sensing data collections, in: Proceedings of the 8th International Conference on Pervasive Computing, in: Pervasive'10, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 138–155.

[106] K. Zheng, M. Li, H. Jiang, K. Zheng, M. Li, H. Jiang (Eds.), Mobile and ubiquitous systems: computing, networking, and services - 9th International Conference, MobiQuitous 2012, Beijing, China, December 12-14, 2012. Revised Selected Papers, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 120, Springer, 2013.

[107] H. Amintoosi, S.S. Kanhere, Providing trustworthy contributions via a reputation framework in social participatory sensing systems., CoRR abs/1311.2349 (2013).

[108] L. Page, S. Brin, R. Motwani, T. Winograd, The pagerank citation ranking: Bringing order to the web, 1999.

[109] H. Amintoosi, S.S. Kanhere, A trust-based recruitment framework for multi-hop social participatory sensing, in: Proceedings of the 2013 IEEE International Conference on Distributed Computing in Sensor Systems, in: DCOSS '13, IEEE Computer Society, Washington, DC, USA, 2013, pp. 266–273.

[110] D. Chaum, Blind signatures for untraceable payments, in: Advances in cryptology, Springer, 1983, pp. 199–203.

[111] A. Jøsang, An algebra for assessing trust in certification chains., in: NDSS, 99, 1999, p. 6th.

[112] L. Kazemi, C. Shahabi, Tapas: trustworthy privacy-aware participatory sensing, Knowl. Inf. Syst. 37 (1) (2013) 105–128.

[113] L. Kazemi, C. Shahabi, A privacy-aware framework for participatory sensing, ACM SIGKDD Explor. Newslett. 13 (1) (2011) 43–51.

[114] O. Hasan, L. Brunie, E. Bertino, N. Shang, A decentralized privacy preserving reputation protocol for the malicious adversarial model, IEEE Trans. Inform. Forensics Secur. 8 (6) (2013) 949–962.

[115] O. Hasan, L. Brunie, E. Bertino, Preserving privacy of feedback providers in decentralized reputation systems, Elsevier: Comput. Secur. 31 (7) (2012) 816–826.

[116] D. Christin, C. Rosskopf, M. Hollick, L. Martucci, S. Kanhere, Incognisense: an anonymity-preserving reputation framework for participatory sensing applications, in: IEEE International Conference on Pervasive Computing and Communications (PerCom), 2012, pp. 135–143.

[117] J. Camenisch, M. Michels, A group signature scheme with improved efficiency, in: Advances in CryptologyASIACRYPT98, Springer, 1998, pp. 160–174.

[118] L. Sweeney, k-anonymity: a model for protecting privacy, Int. J. Uncertain., Fuzziness Knowl.-Based Syst. 10 (05) (2002) 557–570.

[119] J. Camenisch, A. Lysyanskaya, An efficient system for non-transferable anonymous credentials with optional anonymity revocation, in: Advances in CryptologyEUROCRYPT 2001, Springer, 2001, pp. 93–118.

[120] C. Rackoff, D.R. Simon, Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack, in: Advances in CryptologyCRYPTO91, Springer, 1992, pp. 433–444.

[121] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2) (2007) 618–644.

[122] G. Muraleedharan, A. Rao, P. Kurup, N.U. Nair, M. Sinha, Modified Weibull distribution for maximum and significant wave height simulation and prediction, Coastal Eng. 54 (8) (2007) 630–638.

[123] Y. Najaflou, B. Jedari, F. Xia, L.T. Yang, M.S. Obaidat, Safety challenges and solutions in mobile social networks., CoRR abs/1310.5949 (2013).

[124] M.R.P. Gonçalves, E. dos Santos Moreira, L.A.F. Martimiano, Trust management in opportunistic networks, in: Networks (ICN), 2010 Ninth International Conference on, IEEE, 2010, pp. 209–214.

[125] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, P. Yi, Security and trust management in opportunistic networks: a survey, Secur. Commun. Netw. 8 (9) (2015) 1812–1827.

[126] S. Trifunovic, F. Legendre, Trust in opportunistic networks, Comput. Eng. Netw. Lab. (2009) 1–12.

Hayam Mousa is Assistant lecturer at Faculty of Computers and Information (FCI), Menoufia University, Menoufia, Egypt. She received her B.Sc. degree in 2006, Information Technology Department, Faculty of Computers and Information. She prepared her graduate studies and received her M.Sc. in 2011 at Menoufia University, Shiben El-Kom, Egypt. She has a scholarship to complete her Ph.D. studies in France in the beginning of 2014. She works now toward Ph.D. degree at the Institute National des Sciences Appliquées (INSA), University of Lyon, France.

Sonia Ben Mokhtar is a CNRS researcher at the LIRIS lab, in the DRIM group, since October 2009. Before that, she was a research associate at University College London (UCL) for two years, working with Licia Capra. She received her Ph.D. in 2007 from University Pierre et Marie Curie (Paris 6), which she did under the supervision of Valérie Issarny and Nikolaos Georgantas in the INRIA ARLES project-team. Her research interests include Reliable Distributed Systems and Middleware for Mobile Environments. She also a member of the program committees of ICAC 2015, IPDPS 2015, Middleware 2014, IPDPS2014, SOSE 2014 and Compas 2014.

Omar Hasan is Assistant Professor at the Institut National des Sciences Appliquées (INSA), University of Lyon, France. His research interests include distributed systems, information privacy, and trust and reputation management. He received his Ph.D. in computer science from INSA, University of Lyon. Prior to his current position, he was a researcher on the SOCEDA project of the French Agence Nationale de la Recherche (ANR). Additionally, he was a visiting researcher at Purdue University, USA for approximately one year. He also holds four years of software engineering and R&D experience in the IT industry.

Osama Younes is a lecturer in the department of Information Technology at Faculty of Computers and Information, Menoufia University. He received the B.Sc. degree in Electronics Engineering from Menoufia University, Egypt. He received his M.Sc. in performance engineering of systems in 2006 from Menoufia University. In 2013, He received his Ph.D. in Computing Science from Newcastle University, UK. His thesis work focused on modeling, analysis and optimization of mobile ad hoc networks. His main research interests lie with the performance engineering of computer systems, wired and wireless networks, and mobile communication, cloud computing, information and network security, and artificial intelligence.

Mohiy Hadhoud has been a Professor in the department of Information Technology at Faculty of Computers and Information, Menoufia University since 2001. He was the Dean of the Faculty of Computers and Information, Menoufia from August 2008 to November 2010. He also was the vice president of Menoufia University from October 2011 to December 2013. Now, He is the Dean of The Canadian high institute for engineering and business technology (CIC) – new Cairo, Egypt. His research interests include image processing, software engineering and communication networks.

Lionel Brunie is Professor at the Institute National des Sciences Appliquées (INSA), University of Lyon, France since 1998. He was previously a faculty member at the Ecole Normale Supérieure (ENS), Lyon, France. He received his Ph.D. in computer science in 1992 from Joseph Fourier University, Grenoble, France. In 1999, he created the INSA e-learning department which he led until 2002. Then from 2002 to 2006, he headed the Lyon doctoral school in computer science (300+ registered Ph.D.students). In 2003, he co-founded the LIRIS lab in which he acted as deputy director in 2006–2007. In 2007, he co-founded the international doctoral college in “Multimedia Distributed and Pervasive Secure systems (MDPS)”. He leads the LIRIS DRIM research team which comprises of 10 permanent researchers and 20+ Ph.D. students. His main topics of interest include security and privacy, data management in large scale and pervasive systems, collaborative information systems, and e-health applications. He has led numerous national and international research projects; he is the (co-)author of over 180 research papers; he has been member of over 70 scientific conference and workshop committees.